Global Information Assurance Certification Paper

FIBER OPTICS AND ITS SECURITY VULNERABILITIES

GIAC Security Essentials
Certification (GSEC)
Practical Assignment – Version 1.4c
February 17, 2005

Option 1 - Research on Topics
In Information Security

Submitted by: Kimberlie Witcher
Location: University Mary Washington – MBUS 511

TABLE OF CONTENTS

Fiber Optics and its Security Vulnerabilities

Abstract

Bandwidth, performance, reliability, cost efficiency, resiliency, redundancy, and security are some of the demands placed on telecommunications today. Since its initial development, fiber optic systems have had the advantage of most of these requirements over copper-based and wireless telecommunications solutions. The largest obstacle preventing most businesses from implementing fiber optic systems was cost. With the recent advancements in fiber optic technology and the ever-growing demand for more bandwidth, the cost of installing and maintaining fiber optic systems has been reduced dramatically. With so many advantages, including cost efficiency, there will continue to be an increase of fiber optic systems replacing copper-based communications. This will also lead to an increase in the expertise and the technology needed to tap into fiber optic networks by intruders. As ever before, all technologies have been subject to hacking and criminal manipulation, fiber optics is no exception. Researching fiber optic security vulnerabilities suggests that not everyone who is responsible for their networks security is aware of the different methods that intruders use to hack virtually undetected into fiber optic cables.

With millions of miles of fiber optic cables stretching across the globe and carrying information including but certainly not limited to government, military, and personal information, such as, medical records, banking information, driving records, and credit card information; being aware of fiber optic security vulnerabilities is essential and critical. Many articles and research still suggest that fiber optics is expensive, impractical and hard to tap. Others argue that it is not only easily done, but also inexpensive. This paper will briefly discuss the history of fiber optics, explain the basics of fiber optic technologies and then discuss the vulnerabilities in fiber optic systems and how they can be better protected. Knowing the security risks and knowing the options available may save a company a lot embarrassment, time, and most importantly money.

Brief history of fiber optics

In 1870, John Tyndall experimented with a stream of water and a beam of light. He concluded that light uses the waters' internal reflection values to follow a defined path. He demonstrated that the water exiting the small orifice of the first spout combined with a directed beam of sunlight into the stream caused the light to follow a zigzag pattern within the curving path of the water stream. This was the first documented experiment and research into the guiding and transmitting of light (Goff, 2002).

Ten years later, in 1880, Alexander Graham Bell invented the photophone, which transmitted the human voice 200 meters using free-space light as a carrier. Today, over 120 years later, free-space optical connections are widely used in metropolitan networking applications. Between 1880 and 1950, fiber optic technology did not appear to have benefited from any significant advances. In the 1950's, Brian O'Brien and Narinder Kapany, introduced the fiberscope. The new device was the first known use of practical all-glass fiber. Long transmissions could not be achieved due to the fact that the fiberscope experienced a large amount of optical loss, (the loss of signal as it travels). In 1956, Narinder Kapany first coined the term "fiber optics" (Goff, 2002).

The next advancement that played an important part in getting fiber optics to where it is today was laser technology. The light-emitting diode (LED, class II laser) or its higher-power counterpart, the laser diode (Class I laser) were t he only technologies readily available with the potential to generate sufficient amounts of light in a spot small enough to be functional for fiber optics. Today, semiconductor lasers are the ones most frequently used in fiber optics. Optical loss, which keeps the signal from transmitting long distances and impurities in the glass, were two of the biggest challenges facing fiber optics from becoming what it is today. In 1970, Dr. Robert Maurer, Donald Keck, and Peter Schultz of Corning resolved the problem with the impurities in the glass, which brought the attenuation to less than 20 db/km. Fiber optics was now ready for real world applications (Goff, 2002).

In the 1970's, the U.S. military began using fiber optic technology for telephone communications and other applications. Next, came the commercial applications from companies such as, GTE and AT&T. Chicago was one of the first cities to use a fiber optic telephone system. One strand of fiber was able to replace up to 1000 copper cables. This allowed for a dramatic increase in the number of phone calls that could be simultaneously managed. Today, millions of miles of fiber optic cable is used across the globe for transmission of voice, data, video, and other applications. Fiber optic networks are the backbone of the Internet and the backbone of our enterprise communications infrastructure.

Benefits of Fiber Optics

Fiber optic cables have been replacing traditional copper and coaxial cabling for several years. The limitations of copper and coaxial cable cannot keep up with the ever-increasing demands of distance, bandwidth, and real estate. The potential bandwidth of fiber has not been fully utilized and it is already transmitting signals at multiple gigabits per second. Fiber optic cables can go an average of 62 miles versus 1.2 miles that copper can go before the signal needs to be regenerated or boosted. Overall, it is apparent that fiber optics is a more cost effective solution.

Fiber optics is non-metallic and is not susceptible to interference, such as,

electromagnetic interference (EMI), radio frequency (RF) or lightning. Fiber does not conduct electricity. This means that fiber can be installed in many more types of areas that are prone to such interferences. Fiber is also typically smaller and lighter in weight and is practically impervious to outdoor atmospheric conditions. There is no electrical radiation from fiber, making it harder to tap than copper. There are also no issues with grounding, shorting, or crosstalk of cables.

What is Fiber Optics?

Fiber optics is the method of using very thin strands of glass or plastic to transmit communication signals. The cable is light-based, which means data can be sent through at the speed of light, making it capable of handling vast amounts of data in a much shorter time than copper cable. These light signals use the various colors of light (frequencies) as carriers of data. Each color of light can have multiple hues (sub-frequencies) as separate carriers also. These light signals can carry information for thousands of miles. One strand of fiber carries as much information as 1000 copper cables, making it a more efficient and cost effective method of transmitting data over long distances (Fiber Optic Association 2004).

Generally, fiber optic cable consists of a core, cladding, buffer coating, strength member, jacket and an optional armor layer. The core is the center of the cable where one will find hair thin strands of glass or plastic. The core is what carries the optical data signals from the transmitting end to the receiving end. Fiber optic cable is sized in accordance with the cores diameter. The most common sizes are 50-, 62.5-, and 100-micron Gable, although 100 are not used as much today. As the core size gets larger, the cable is able to carry more light.

The purpose of the cladding is to trap the light in the core by using the principal of total internal reflection. The cladding is made up of a material that is of a lower index of refraction than the core. The light is reflected back into the core due to this lower index.

The buffer, also called a coating, helps protect the fiber from physical and environment damage. The buffer is commonly made of a gel material or a thermoplastic material. The coating is stripped away from the cladding to allow termination to an optical transmission system during installation.

The strength member is usually made up of Kevlat4, wire strands or gel-filled sleeves. Its purpose is to protect the cable during installation or times of excessive tension.

The outer layer of the cable is called the jacket. The jacket is usually orange in color and serves to protect against contaminants.

The optional outer layer of the cable is called the armor. This layer is usually metallic, rigid, weatherproof, and very strong. It serves as a physical security measure against outside forces or manipulation.

A fiber optic transmitter, cable, and receiver are needed for a successful fiber optic transmission. The transmitter converts the electrical signal into an optical signal. The cable carries the light transmission from the transmitter to the receiver. The receiver uses a photodiode or photocell to detect the light, and then converts the light transmission back to an electrical signal. For longer distances, an optical regenerator may be needed to boost a weakened signal (lightspeed, MPBS).

Outside Plant and Premise Installation

Fiber optics used in telephone networks, CATV or outdoors is referred to as "outside plant". Outside plant fiber is almost always single-mode fiber and can contain up to 288 fibers per bundle. The fiber is typically located "outside", whether it is run through a conduit, hanging from a pole, underwater, or underground. Outside fiber can run for a short distance or up to hundreds of miles. Easy access to "outdoor" fiber can cause security issues. If an intruder has access to your fiber cable, they can use one of several methods to tap the cable and gain access to all data traversing the cable. However, it is not always practical or cost effective to encase all outside fiber in concrete or to make sure all access to the cable is restricted. Utilizing very strong encryption methods may help reduce this area of security concern, but will not alleviate the problem.

Premise fiber is used mostly in buildings or on campuses. Each cable carries a significantly smaller amount of fibers, typically between 2 and 48 fiber strands per bundle. This type of fiber installation involves shorter lengths and mostly "multi-mode" fiber (Fiber Optic Association, 2004). It is easier to ensure that access to the premise fiber is restricted, but necessary security measures are not always exercised in these environments. Special attention should be paid to places where fiber is accessible, such as, wiring closets, crawl spaces and ducts.

Single-mode and Multi-mode

The two most popular types of optical fibers are single-mode and multi-mode. Single-mode fiber is used for long distances and has transmission rates up to 50 times more distance than multi-mode. This technology uses the more powerful laser diode and can transmit infrared laser light in wavelengths 1300nm or 1550nm (LightSpeed MPBS). It only has one mode of transmission and costs more than multi-mode, but it is less susceptible to signal attenuation and distortion from overlapping light pulses. The core itself is small, about 9

microns. Single-mode also has a small numerical aperture (NA). A smaller NA requires more precise work to splice a cable. Splicing can be used as a method to extract data directly from the cable for legitimate and non-legitimate reasons.

The core diameter of mulit-mode fibers is usually 50, 62.5, or 100 micrometers. Multi-mode fiber transmits data using the less powerful LEDs (light-emitting diodes) transmits infrared laser light in wavelengths 850nm or 1300nm (LightSpeed MPBS). As the name implies, transmission occurs in more than one mode as light waves are dispersed through the cable. This type of cable is great for medium to short distances. Multi-mode fiber can be used with less expensive connectors and LED transmitters, making it a more economical choice for applications with shorter distances and lower bandwidth demands (ARC Electronics).

Index of Refraction (IOR) and total internal reflection

Before we discuss the security vulnerabilities of fiber optics, it is important to understand the concept of index of refraction (IOR) and total internal reflection. It was stated earlier that since the cable is light based, data travels at the speed of light. The speed of light in a vacuum is 186,000 miles per second. When the light is traveling through a medium, the speed is different to that of light traveling through a vacuum. The index of refraction is found by dividing the speed of light in a vacuum by the speed of light in a medium. By definition, the IOR of a vacuum has a value of 1. The typical IOR for the core is 1.48 and 1.46 for the cladding. Light travels slower in the medium, as the IOR gets larger. (Alwayn, 2004)

For fiber optics cables to successfully transmit data, a process called total internal reflection must occur. By definition, total internal reflection is "when a light ray traveling in one material hits a different material and reflects back into the original material without any loss of light" (Corning Incorporated, 2005). This is what happens with the core and cladding inside a fiber optic cable. The IOR of the core is higher than that of the cladding, so when the light from the core hits the cladding it is reflected back to the core and the data continues to travel. The index of refraction for the core must be higher than the cladding in order for total internal reflection to occur. If the IOR was lower in the core, all of the light would not be reflected back to the core and you would have a loss of light, thus a loss of data.

Fiber optic cable has a critical angle at which light must enter. Measuring from the normal or cylindrical axis of the core, apply the following formula: qc = cos-1 (n2/n1). The IOR of the cladding is represented with n2 and the IOR for the core is represented with n1. For example, if we replace n2 with 1.46 and n1 with 1.48, our critical angle would be 9.43 degrees (Alwayn, 2004).

If the angle of incidence is greater than the critical angle, then there will be no

angle of refraction. This means that if the light entering the cable hits the core-to-cladding interface at an angle greater than the critical angle it will be reflected back to the core, if it hits at angle less than the critical angle, attenuation occurs and the full signal will never reach the receiver. Attenuation in fiber optics can be explained as the loss of optical power as the light makes its way down the cable. If the light hits impurities in the glass, it will scatter or be absorbed. Extrinsic attenuation may be caused by microbending or macrobending (Alwayn, 2004). The loss of photons from microbends and macrobends can be used to an intruder's advantage.

Security Concerns

Each year companies spend billions of dollars securing their networks and each year billions of dollars are lost due to intrusion into those same networks. At first, fiber optic networks were touted as one of the most secure infrastructure options. In the last couple of years, it has been suggested that fiber is almost as easy to tap as copper. Today, there are millions of miles of fiber cable spanning across the globe. There is an unimaginable amount of data being transmitted across these cables daily including sensitive government data, personal, financial and medical information. If wiring is in a public access space, this data may be compromised. Tighter access control to the cabling needs to be implemented. More companies need to employ physical layer security systems in conjunction with their existing data layer security systems. Physical layer security systems are more able to detect and deal with intrusions to the cables that do not involve an easily measurable amount of data interruption. Also, it may not be completely advantageous to post fiber optic communication infrastructures on the Internet. This can provide a roadmap and bring attention to fiber optic communications vulnerabilities.

Once an intruder has gained access to the cable, the actual tap is believed to be easier to accomplish than once thought. To do a virtually undetected tap, it is almost certain that intruders would only need available commercial items, such as, a laptop, optical tap, packet-sniffer software, and an optical/electrical-converter. When a successful tap is made, the packet-sniffer software can filter through the packet headers only. This means that filters can be applied to the data allowing specified IP addresses, MAC addresses or DNS information to be gathered and then stored or forwarded to the intruding parties various tools and mechanisms, including other optical connections, links , wireless, another wavelength or other resources (Oyster Optics Inc, 2003).

If an intruder is successful in using an unobtrusive method to retrieve data directly from the fiber optic cable, then the intruder does not need access to the company's network. Thus, there are no worries on how to get around firewalls, most IDS, or IPS. If the company is encrypting their transmitted data, this may provide a stumbling block for the intruder. Depending on the encryption methods used, it may still only be a matter of time before the intruder breaks the

encryption and has their desired data.

Other types of optical taps

Splicing a fiber optic cable is detectable by most network security systems, but it is the easiest method and may still be used from time to time. When performing an optical tap using the splice method, there is a brief interruption of data. If this disruption of service is noticed, a technician or repair person will be sent out to find the source of the disruption. Thus, it can be a short-lived tap and is not the preferred method.

A fiber optic cable can be tapped without actually piercing the fiber or disrupting the flow of the data. Fiber can be bent or clamped in a precise way that will form micro-bends. When micro-bends or ripples are introduced, photons of light will leak out and there is a possibility that the intruder's receiver can capture enough of these escaped photons of light to have viable data (Oyster Optics Inc, 2003). This method appears to be more successful at lower speeds and not effective on higher data rates.

In the article "Fiber Optic Taps Backgrounder", by Oyster Optics, it is explained that even a signal leak of less than 0.1dB contains all of the information being transmitted by each photon. Once the signal is captured, the intruder can use an optical fiber network analyzer to determine the communications protocol and to decipher the information. All the while, there is no disruption or indication of interference with the end users communication, thus the tap is virtually undetected (Oyster Optics Inc, 2003).

According to the same source, there are available methods that can be used to tap fiber cable without actually physically touching the cable. These non-touching active taps inject additional light into the fiber plant and analyze the underlying optical signal by gauging certain interactions between the two. Without the right kind of physical-layer optical signal protection, an end-user may never notice that their data is being intercepted. It also indicates that another vulnerable concern is when intruder gains access to the cable before the first switching center. Detection can go unnoticed and optical tapping requires less complex and expensive equipment in the local and access loops (Oyster Optics, 2003).

There have been several patents awarded that discuss additional methods for optical taps. One is U.S. Patent 6,265,710 which was awarded to Herbert Walter on July 24, 2001. "*Method and device for extracting signals out of a glass fiber*". Complete patent information can be found at: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=6,265,710.WKU.&OS=PN/6,265,710&RS=PN/6,265,710

A second patent, U.S. Patent 6, 535,671 was awarded to Craig D. Poole on March 18, 2003. "*Optical fiber taps with integral reflecting surface and method of making same."* Complete patent information can be found at: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=6535671.WKU.&OS=PN/6535671&RS=PN/6535671

Fiber Optic Security Counter Measures

Foptic Secure Link, developed by the Australian firm Future Fiber Technologies Pty. Ltd., can be used for sensing physical disturbance. It uses a technology that can concurrently make use of a fiber optic communications cable as a tampering-alert, intrusion-alert, or integrity-testing sensing cable. It monitors in real-time any physical disturbances, such as clamping or bending. One key advantage to using this technique is that it is not necessary for optical losses to occur in order for the technique to sense disturbances (Tapanes and Carroll).

A second method is the encryption method of the data being transmitted. Very strong encryption with long codes should be used. An end user may also try using a physical method that changes the light signals as it simultaneously identifies illegal attacks. This is explained in U.S. Patent 6,469,816 (Snawerdt 2002).

The January 2005 issue of *"Discover"* contains an article about using photons to encrypt data. The process mentioned is described below:

A transmitter sends photons that are specifically directed at given intervals through a fiber optic cable. The receiver then analyzes the arrival of the photons at the given intervals. When a matching segment of the transmission pattern, which is advertised on a separate wavelength by a transmitter, is received, the receiver will then utilize this "key" and authenticate the unlocking of the data from the stream. The light beam passage is so weak that any alteration would be immediately observed; any intruder snooping or injecting would inevitably disturb the photons pattern. The receiver's device would detect the change in pattern, ending the transmission and sounding the alarm. The article goes on to mention that since the signals are weak, the range is about 60 miles and this method would require its own freestanding fiber optic network (Svoboda 33). It may not be a viable option right now, but it will be interesting to see where it takes us in the future of information security.

Opterna's FiberSentinel System uses WaveSense intrusion prevention technology, artificial intelligence, and optical digital signature recognition to monitor fiber connections. It reportedly detects all physical intrusions and

immediately cancels all transmissions. At the time of intrusion detection, this continuous real-time monitoring system will switch the data transmission to an alternate fiber path and alerts the network operator (Book, 2002).

Oyster Optics, Inc. reports that it has developed an optical security, monitoring, intrusion detection solution that is protocol independent. The system uses a secure phase modulation of the optical signal to impress data on the optical carrier. If data is intercepted, the intruder will not be able to gain access to captured data unless they happen to have a receiver provided by Oyster Optics' that is synchronized to the transmitter at power up. Oyster Optics' provides a unique transmitter and receiver by using a non-pseudo-random manufacturing process that cannot be replicated. This system will also reroute data transmissions to a backup system when an intrusion is detected. There solutions can be implemented as a stand-alone device or at the transceiver card level (Oyster Optics, 2003).

Conclusion

Intruders can tap fiber optic systems virtually undetected using several different methods. It may not be a completely simple task, but with the right equipment, knowledge and access, it could probably be achieved by a mid-level hacker. It is alarming that there appear to be many organizations out there who are not aware and do not agree on the ever increasing ease at which fiber optic cables can be attacked. There are still many current data layer intrusion systems that are not designed to detect some of the more unobtrusive optical tapping methods. Several companies have demonstrated the importance and effectiveness of adding a physical layer security system to an organizations existing network security system in order to detect and deal with more of these types of intrusions the moment they happen. Data security will always be a problem. Intruders not only have a variety of reasons for stealing or manipulating data, but also a variety of methods to obtain the data. Constant and up to date awareness and knowledge of the current risks and solutions is essential to ensure that all data is as secure as technically and financially possible.

Works Cited

Alwayn, Virek. "The Physics behind fiber optics". Fiber-Optic Technologies. 23 April, 2004. URL: http://www.ciscopress.com/articles/article.asp?p=170740&seqNum=3

ARC Electronics. " Brief Over View of Fiber Optic Cable Advantages Over Copper". The basics of Fiber Optic Cable – a Tutorial. Date unknown. URL: **http://www.arcelect.com/fibercable.htm**

Book, Elizabeth. "Info-Tech Industry Targets Diverse Threats. Fears of network vulnerability fuel market for improved security systems". August 2002. URL: http://www.americantechsupply.com/fiberopticsecurity.htm

Corning Incorporated. "Basic Principles of Fiber Optics", Corning Cable System. Author unknown. 2005. URL: http://www.corningcablesystems.com/web/college/fibertutorial.nsf/appprin?OpenForm

Goff, David R. "A Brief history of Fiber Optic Technology", Fiber Optic Reference Guide, 3rd ed. Focal Press: 2002. URL: www.fiber-optics.info/fiber-history.htm

Fiber Optic Assocation. "Understanding Fiber Optic Communications". 2004. URL: http://www.thefoa.org/ppt/

LightSpeed MBPS, Inc. "Fiber Optics 101". Date unknown. URL: http://www.lightspeed-mbps.com/fiber_optics_101.html

Oyster Optics, Inc. "Securing Fiber Optic Communications against Optical Tapping Methods", White paper on optical taps and various solutions. 2002-2003 URL: http://www.oysteroptics.com/index_resources.html

Poole, Craig D. "Optical fiber tap with integral reflecting surface and method of making same". US Patent 6,535,671. March 2003. URL: http://patft.uspto.gov/netacgi/nph-

Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=6535671.WKU.&OS=PN/6535671&RS=PN/6535671

Snawerdt, Peter. "Phase-Modulated Fiber Optic Telecommunications System". US Patent 6,469,816. October 2002. URL: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=6469816.WKU.&OS=PN/6469816&RS=PN/6469816

Svoboda, Elizabeth. "Code Breakers Stumped by Photon-Based System." Discover January 2005. 33 Vol 26, No.1

Tapanes, E and Carroll, D. "Securing Fiber Optic Communication Links Against Tapping", Foptic Secure Link – White paper. Date unknown. URL: http://www.fft.com.au/products/FOSL_WP.PDF

Walter, Herbert. " Method and device for extracting signals out of glass fiber" US Patent 6,265,710. July 2001. URL: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=6,265,710.WKU.&OS=PN/6,265,710&RS=PN/6,265,710