Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.4, No.4, 2014

The Vulnerability of Fiber-Optics Communication Systems: The Role of Optical Tapping

UMOH, GABRIEL ETIM
DEPARTMENT OF ELECTRICAL/ELECTRONIC/ICT ENGINEERING
FACULTY OF ENGINEERING, AKWA IBOM STATE UNIVERSITY
IKOT AKPADEN, MKPAT ENIN LGA
AKWA IBOM STATE, NIGERIA
E-mails: gabriel.umoh5@gmail.com

AKPAN, ANIEFIOK OTU
DEPARTMENT OF PHYSICS
FACULTY OF NATURAL AND APPLIED SCIENCES,
AKWA IBOM STATE UNIVERSITY
IKOT AKPADEN, MKPAT ENIN, L.G.A.
AKWA IBOM STATE, NIGERIA
E-mails: aniefiokotu@gmail.com

ABSTRACT
Optical tapping devices placed in public and private optical networks today allow unfettered access to all communications and information transiting any fiber segment. Available legally and inexpensively from numerous manufacturers worldwide, optical taps are standard network maintenance equipment that are in use daily. When used nefariously, optical taps provide an excellent method of intercepting voice and data communications with virtually no chance of being detected. Intruders are therefore rewarded with a bounty or relevant information while subject to a very low risk of being caught. Optical network equipment manufacturers do not currently incorporate adequate protection and detection technologies in their platforms to monitor such network breaches in real-time. Network operators thus cannot safeguard the optical signals on their networks and therefore cannot prevent the extraction of sensitive data and communications. Government networks, while assuredly more secure, are also vulnerable to certain type of advanced passive and active tapping methods. This background paper serves to provide an overview of the vulnerabilities of today's modern optical networks; describe methods of addressing such issues; and introduce optical security, monitoring, intrusion detection and breach localization solutions.
Keywords: Fiber optics, optical tapping, splitters, couplers, optical time domain reflector (OTDR), Oyster optics.

1.0 Introduction

Fiber optic telecommunications systems make up the backbone of all modern communications networks. Whether voice, data, video, fax, wireless, e-mail, TV or otherwise, over 180 million miles of fiber optic cables worldwide transport the ever-increasing majority of our diverse information and communications. Modern economies and societies rely on the availability, confidentiality and integrity of critical fiber optic network infrastructures to function properly and efficiently.

With the initial introduction of fiber optic telecommunications systems came the belief that fiber-based transmissions are inherently secure. It has since been proven that not only are fiber optic systems simples simple to tap than their copper-based predecessors. Furthermore, tapped optical networks divulge much greater pertinent information in a more orderly and digitized manner. In fact, many fiber optic taps are standard network maintenance equipment used daily by carriers worldwide. Used illicitly, however, such devices allow the extraction of all voice and data communication in the fiber plant with little or no chance of detection.

2.0 Methodology

This is achieved because the light within the cable contains all the information in the transmitted signal and can be easily captured, interpreted and manipulated with standard off-the-shelf tapping equipment. Private and public networks today do not incorporate methods for detecting optical taps in real-time, offering an intruder a relatively safe data extraction proposition. As fiber optic systems transmit large volumes of data as light within an optical fiber, such methods are thus a preferred low-risk method of intelligence gathering, reaping access to large amounts of information. From an eavesdropping and espionage point-of-view the benefits are obvious.

Today, we live in a society where corporate espionage has become an international sport. As communications using fiber optics become increasingly ubiquitous, so too does the potential for the illegal tapping and stealing of confidential and commercially sensitive data. It is estimated that over $100 billion was

lost to U.S. companies alone in 2000 due to corporate espionage activities, whereas $20 billion was lost through purely technical means. Internationally over 100 foreign government agencies routinely obtain and provide sensitive information on companies to their own domestic firms. In fact, is the most recent *Federal Bureau of Investigation and Computer Security Institute* "2002 Computer Crime and Security Survey", major U.S. companies and organizations stated that their most likely source of attack was from combined espionage activities stemming from U.S. competitors, foreign corporations and foreign governments. Independent hackers and disgruntled employees, while always a danger that must be appropriately managed, ranked second and third behind the combined threats of espionage. Recent examples include French taps on UK wireless networks for executive conversations in competitive bidding situations; taps placed by criminals in Dutch police networks; optical taps placed by the former East German Secret Police (STASI) on the optical links between West Berlin and West Germany; and even the recent tapping of the optical lines of a major Boston-based financial institution.

Particularly problematic is the fact that the vast majority of optical taps persist completely undetected, as carriers and most enterprises today do not employ adequate techniques to monitor, detect and protect data on their optical networks. Clearly in such an environment, fiber optic networks, which are the lifeblood of all communications and data transfer in modern society, are real target for attacks.

Traditionally illegal entry into systems has been through taping into communication systems or intercepting radio transmissions. In recent years, however, the general population has been much more focused on computer hacking. Hackers have different goals and tend to wish that the success of their intrusion exploits become well known to the public. Such high-profile attacks, such as Denial-of-Service attacks or the "I-Love-You" virus, attract much media attention. While they do have financial repercussions for the victims, they pale in comparison to the massive losses that can stem long-term form undetected fiber optic taps that may remain in place for extended periods of time and provide accesses to all of a corporation's information and communication transiting to and from a facility, building, campus or region.

In comparison, professionals have a very different modus operandi, as they wish to extract as much information for as long as possible for a specific financial or political gain and with the goal of not being detected or caught. Fiber optic taps provide a very useful method in their arsenal of illicit information gathering tools.

As a result, contrary to popular belief, fiber optic telecommunications systems are extremely vulnerable to being tapped and few private or public network operators, if any, can claim that their networks are 'tap free' or protected even minimally from optical tapping methods.

3.0 FIBER OPTIC COMMUNICATIONS

Optical fibers are dielectric wave guiding devices used to confine light. These cables are typically constructed of silica glass cores surrounded by a cladding, which is then protected by a jacket. While cladding is typically also made from a silica glass, some applications utilize plastic or "doped" silica. Regardless of material, in order for internal refraction and propagation of the light through the optical fiber, the cladding's refractive index must be lower than the core to satisfy Snell's Law. The primary function of the jacket is to protect the fiber from damage.

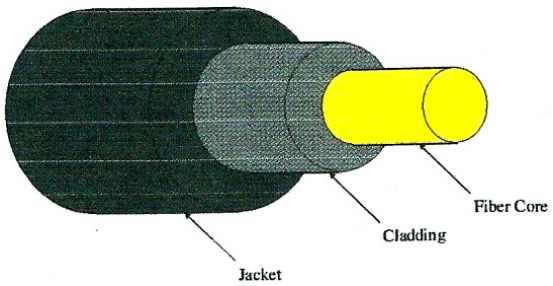


Figure 1: Standard cross-section view of an optical fiber

Communications using optical fibers have several attractive features and advantages over other communications systems. These advantages include:

- Greater bandwidth and capacity
- Electrical isolation

- Low error rate
- Greater immunity to external influences
- Greater immunity to interference and crosswalk.

Fiber optic communication systems have been increasingly deployed in telecommunications systems, as their high bandwidth has allowed them to replace copper at an initial rate, for example, of approximately one fiber cable for each one thousand copper wires. Advances in DWDM have continued to push such ratios even further through additional wavelengths and channels.

With such popular properties, it should come as no surprise that optical fibers have become the most affordable and efficient means of transmitting information over communications systems.

The increased capacity and growth of overall bandwidth has allowed for the tremendous grow of other communications media, such as wireless networks, the internet, corporate Wide Area Networks, Storage Area Networks, and the like, which all utilize fiber optic cores. Fiber-based communications systems have thus replaced virtually every prior type of communications system at the core and as they continue expanding to the edge of the network, it is indeed only a matter of time before optical fibers reach nearly every desktop and most homes. Further advances in all-optical switching and even early developments in optical processors and busses promise a future teeming with all-optical, land-based network infrastructures.

4.0 The Vulnerability of Fiber Optic Communication Systems

Modern fiber networks deploy over 180 million of miles of fiber worldwide. These networks allow for the transmission of large amounts of data and information from point-to-point cheaply and easily, and carry extremely important and confidential information. Although it was initially though that these fiber optic systems would be inherently secure, it has been discovered that the extraction of information from optical fibers is relatively simple and is aided by the increasing sophistication and availability of standard test and maintenance equipment.

There are various fiber optic tapping methods, but most fall into the following main categories:

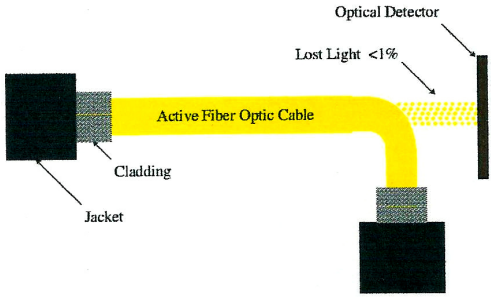
- Splice
- Splitter or Coupler (Variable)
- Non-touching method (passive and active)

4.01 SPLICE:

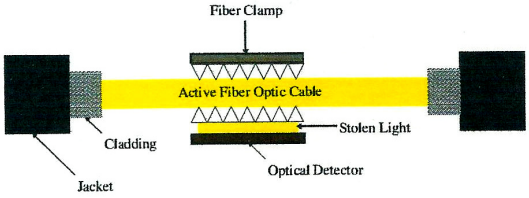
The simplest method of tapping is by splicing the optical fiber briefly and inserting equipment to allow for the signal to transit to the end party while also being intercepted by the intruder. Optical splices do provide a momentary lapse of data while the fiber is no operational. Carriers do not, however, have the real-time ability to locate fiber breaks and must then usually roll-out trucks, technicians and insert additional external equipment. Thus, if downtime is short, many operators 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, however, does not interrupt the signal and thus the splicing method is not preferred.

4.02 Splitters and Couplers (Variable):

Such methods allow the tapping of an optical fiber without actually breaking the fiber or disrupting the data flow. One of the lesser-known properties of optical fibers is that light is easily lost from both the jacket and the cladding of the fiber, particularly if the fiber is bent, or clamped, in such a way that micro-bends or ripples are formed in its surface. Perhaps the simplest example of such phenomena is that one is able to see the light in an optical fiber if one holds an optical fiber in one's hands. Just as simply as one sees the light (as one's eyes are after all biological optical detectors), so does the equipment designed to interpret it. In reality, all that is required to extract all of the information traveling through an optical fiber is to introduce a slight bend into the fiber, or clamp onto it at any point along its length, and photons of light will leak into the receiver of the intruder.



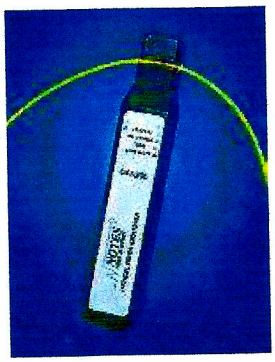
2(a)



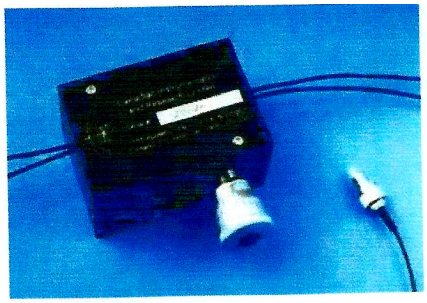
2(b)

Figure 2: Illustrated below are two simple taps that allow for the bleeding of light from the optical fiber.

In fact, many optical fiber test instruments are designed specifically to take advantage of this fact. For example, below is a commonly available optical Fiber Identifier that is used to determine the direction of an optical signal, without the need to remove the jacket. Other passive, non-intrusive tapping devices are also shown.



3(a)



3(b)

3(c)

3(d)

Figure 3(a-d): Commercially available optical signal tapping advice for determining signal direction 3(a), polarization maintaining variable ratio evanescent wave coupler 3(b), micro-bend clamping tapping device 3(c), and macro-bend tapping device 3(d).

For a basic tap, only 0.2 dB of optical power is needed to identify the signal presence and direction. Thus it is quite simple to utilize more sensitive optical detectors and additional electronics to collect the entire optical signals. Once this is accomplished, an optical fiber network analyzer, which is a commonly available test instrument manufactured by a number of companies, may be used to determine the communication protocol and to decipher the information.

Even when only less than 0.1 dB (~2%) of signal is leaking, it will still contain all of the information being transmitted by each photon. The user at the other end will never know that their information has been compromised since they will experience no apparent interference with their communication.

4.03 Network Disruption:

In fact, some tapping device may be utilized not just for passive tapping, but for active tapping, in which there occurs an injection of signals into the fiber plant for various uses, such as legitimate maintenance or even dangerous network disruptions and attacks. Such techniques could be used in order to introduce false information or to corrupt existing information flows. Such capabilities allow a wide range of misuse, ranging from corporate espionage disinformation to terrorist disruptions of the critical communications infrastructure. Unlike blatant physical attacks on the network infrastructure, such as cutting an optical cable, optical taps used in today's networks for disruption purposes are subtle in nature, not detectable in real-time, difficult to locate and reap havoc on infrastructure integrity and availability.

4.04 Non-touch methods (passive and active):

Numerous methods of tapping optical fibers exist without the need to actually touch the fiber or "steal" light from the fiber plant. Some methods, while having been around for over a decade, have recently been published in the public domain and are now accessible worldwide by anyone who has access to an Internet connection. A recent U.S. Patent (6,265,710), as well as European Patent (0 915 356), issued to Deutsche Telekom, describes in detail "a method or device for extracting signals out of a glass fiber without any detectable interference occurring, in particular without the singles propagating through the glass fiber experiencing any transmission loss…"

- While this specific implementation is limited to a maximum bit-rate, other lesser-known methods also exist, which allow for much higher bit-rate optical taps. More notable is that although off-the-shelf equipment for such undetectable optical taps are not currently available for purchase, the patent documents describe clearly the preferred method and how such a device is constructed and operates.

More advanced non-touching active taps in contrast inject additional light into the fiber plan and are able to deduce the underlying optical signal by gauging certain interactions between the two. Such non-touching taps are primarily undetectable and thus, without the proper physical-layer optical signal protection in place, data may be intercepted indefinitely without notice by the network operator or end-user.

Figure 3(e)An example of the tapping of a live video conference over a 10 kilometer span without network disruption or visible signal degradation in a laboratory setting. Intercepted video conference between two laptops replayed on third laptop in real-time

5.0 GOVERNMENT VS COMMERCIAL NETWORK

Commercial fiber optic networks and the equipment that make them possible do not incorporate comprehensive protection mechanisms against optical tapping methods. Intruders utilizing optical taps in commercial networks do so knowing that they can reap an abundance of targeted information in an organized and digitized format with little or no chance of their illicit activities being detected by either the carrier or the carrier's corporate customers.

Government networks, however, do incorporate more robust protections against tapping methods in general. Such efforts depend on the type of network, the importance of data being transmitted, and importance of data being transmitted, and the nature of application. For instance, many government networks prudently encrypt much or all data for transmission. Likewise, some government networks will use random daily Optical Time Domain Reflectometer ("OTDR") scans to look for possible changes in fiber health indicative of possible tapping activities. In such cases non-touching passive and active tapping methods still leave government networks susceptible to eavesdropping, espionage and disruption. More drastic measures such as reinforced concrete conduits or gas-filled packaging may also be used in extreme situations where cost is not a discernable issue.

It should be noted that in all cases government networks are trying to protect against optical tapping methods. Otherwise there would be no reason to undertake such protective measures in the first place.

6.0 Protecting Information

Based on the aforementioned evidence it is easy to conclude that by using relatively inexpensive optic-electronic components widely available in the telecommunications industry, an effective detector to tap an optical fiber can be built or easily purchased preassembled. This has serious security implications for users of fiber optical communication systems, especially those with sensitive data such as financial institutions,

exchanges, insurance firms and healthcare corporations, as well as R & D facilities, global manufacturers, government and other agencies.

Typically sensitive information is believed to be the domain of high security organizations such as the military or foreign affairs departments. In the competitive global marketplace, however, commercial organizations possess and exchange communications and information that is critical to their survival. Much of this data is exchanged or supplied in strict confidence with their clients, partners or global subsidiaries. Such organizations include accounting firms, R & D organizations, government regulatory bodies, and insurance companies to name only a few.

All public and private network operators and their respective clients are completely vulnerable to the tapping and stealing of their mission critical communications and information. The underlying vulnerability of the global optical communications infrastructure has not been publicly raised to-date mainly because suppliers, operators and users have failed to understand the severe threat and because there have been no effective solutions available until recently to counteract such occurrences. Furthermore, suppliers and operators have not yet integrated optical security technologies and thus tapping incidents are rarely detected and never publicized for obvious reasons of brand protection and risk mitigation. The public today is under the false impression that topical fibers are a secure means of communications. This is simply not the case.

Optical networks are particularly vulnerable in the local and access loops and wherever intruders have ample opportunity to access fiber in the public domain or choice spots of weakness. For example, access to fiber cables is plentiful in and around a customer premise, as well as between the customer premise and the first switching centre, typically in the local fiber loop. If accessed before the first switching center, typically in the local fiber loop. If accessed before the first switching center, 100% of all voice and data communications can be typically intercepted and extracted without customer or carrier knowledge. The required equipment for optical taping is also less expensive and complex in the local and access loops, where speeds and network topology are simpler to manage.

In larger cities and financial centers, optical network vulnerabilities are particularly magnified for systems in multi-story, multitenant buildings, such as high-rises, where users often occupy a number of non-adjacent floors. Optical cables linking the telecommunication facilities typically travel in risers or elevator shafts where there is no existing monitoring or security capabilities. Organization simply do not realize that their information and communications are simple to extract via an easily placed tap in such easily accessible common areas.

Telephone closets, cages, conduits, risers, shafts, parking garages, manholes, subways, telephone poles and many other areas are all accessible to place fiber taps. The further trend towards greater globalization only adds to the problem as companies become more competitive and find themselves located on less than familiar foreign soil.

7.0 Solutions

Proactive vs. Reactive: Most security measures today are reactive in nature. That is, they are meant to slow down or hinder an intruder that is trying to penetrate a network through means such as encryption. While such reactive techniques may be successful in deterring many intruders, they do not stop all intruders nor do they allow for the actual interception of the intruder. Thus intruders are not caught and cannot be stopped from pursuing such efforts again in the future

Proactive security measures, however, enable the immediate determination of an intrusion event and can identify the extract location in the fiber plant of the intruder in real-time. Law enforcement and Homeland Security Forces thus have an effective tool to detect and locate intruders during an intrusion attempt while also stopping the perpetrators from future network attacks. Therefore a comprehensive combination of proactive and reactive security methods that not only protect the entire fiber optic carrier signal from eavesdropping, but also allow the interception of intruders, is highly desirable.

Oyster Optics, Inc. had developed and patented groundbreaking optical security, monitoring, intrusion detection and breach localization solutions for today's global optical networks. The company's technologies are encryption-free (yet encryption-compatible), protocol-independent and provide for the highest level of security on already existing optical infrastructures. Because the physical transport layer is completely secured, all higher networking layers and data types are subsequently protected as well. Oyster Optics licenses their unique technologies to telecommunication equipment vendors and defense contractors for implementation in public and private networks. Special configuration for extremely secure government applications and networks are available. Oyster Optics also provides customized design, engineering and support services.

Corporate espionage of all sorts in on the rise with the tapping of fiber optic networks allowing intruders to access all of a firm's voice and data communications all of the time. Offsite co-location, hosting,

back-up, disaster-recovery, and SAN facilities exacerbate this trend and allow increasingly greater opportunity for intruders to access a company's crucial information from the safety of an off-premise network winding through the insecure and open public domain. Today's common security technologies simply do not lock-down the physical transport layer nor do they provide adequate security across the optical network.

Oyster Optics' technologies incorporated into optical equipment for carrier and government networks provide the strongest network security available thus making all data, voice, video, imagery or other information completely unrecoverable to a hostile or unwanted intruder utilizing optical tapping techniques. Intrusion detection and breach localization techniques monitor the fiber optic plant in real-time for intrusions and maintenance events thus allowing for the dispatch of specific resources occur. Global Fortune 1000 corporations, financial institutions, R & D facilities, and government agencies should seek such assurances when linking together their geographically disparate facilities. Any lesser steps are an open invitation for intruders to exploit known network weaknesses.

oyster Optics' technologies provide for the secure transmission of optical voice and data over existing fiber optic networks. Using a patented method of secure phase modulation of the optical signal to impress data on the optical carrier, the data can only be recovered by a specialized Oyster Optics' receiver synchronized to the transmitted at power up. Each Oyster Optics' enabled transmitter and receiver is truly unique through a non-pseudo-random manufacturing process and thus not reproducible. Traditional methods for tapping optical packets and for decoding encrypted data are thus useless in attempts to tap a fiber protected with Oyster Optics technologies. In addition, due to the nature of the optical signal sent using Oyster Optics' patented secure phase modulation technologies, attempts to tap Oyster-protected fiber, along with the attempted tap location in the fiber plant, become immediately known to the network operator via highly-sensitive intrusion detection technologies. The optical signal is thus completely safe from eavesdropping attempts and can be automatically rerouted over another safe Oyster-protected fiber route as warranted.

Oyster Optics' proprietary transmission methods enable new advancements in the areas of optical security, monitoring, intrusion detection and maintenance. Combined together, four primary methods provide an unparalleled level of security against all optical tapping techniques in fiber optical networks:

1. **Physical-layer security:** Completely secures fiber optic transport layers (0, 1) making data virtually impossible to recover and read.
2. **Intrusion Detection:** Highly-sensitive monitoring of various intrusion and maintenance events with fine-tunable thresholds allows immediate alerts of network penetration attempts.
3. **Breach Localization:** Calculates the exact position of such events along optical fibers in real-time. Law enforcement actions against perpetrators are now enabled for the first time through proactive integrated means. Maintenance and repair actions are also more targeted and effective.
4. **Output optimization:** Software management limits the overall available light in a fiber plant to the exact fiber span length. Acceptable signal-to-noise-ratios and bit-error rates are software programmable, allowing for robust optical links while limiting, however, the superfluous light typically found in fiber plants, which would otherwise provided further means of exploit through optical taps.

8.0 Conclusions and Recommendations

Communications are an essential factor in today's modern information technology and service based economies. Global commerce is dependent upon the critical communications infrastructure and relies on that availability, confidentiality and integrity of data and voice transmission. Sensitive communications and information, which are illegitimately extracted from public and private networks, can be used illicitly for financial, political or other gain. Corporate espionage has surpassed government espionage as the primary motivation behind such actions. Global competitors increasingly seek competitive advantage, confidential information, financial gain and proprietary market intelligence through such nefarious means. Terrorism through the disruption or destruction of the integrity and availability of the critical communications infrastructure must be considered as organizations around the world utilize increasingly sophisticated means of attack.

Optical networks have proven adept at transporting massive amounts of information cheaply and efficiently around the world. Today's communication networks of all types consist of fiber optic networks at the core and spreading out towards the edges. Further technological advances and price reductions have brought optical fibers to most corporate buildings and over time are working their way to the final edges of the network, onto the desktop and even into more affluent residential neighborhoods and residences. Today's corporations, and indeed the economies they support, rely heavily upon the communication services provided by optical networks.

Optical tapping methods enable the extraction and sorting of large volumes of voice and data transmitting an optical fiber. Media of all types are essentially digitized, organized and transmitted across optic networks via well documented standardized protocols. The inherent insecurity of fiber optics, and the belief that they are indeed secure, is perhaps one of the greatest misconceptions in the communications industry today.

Corporations, governments and other organizations, which choose to ignore these unseen dangers, stand to face potentially significant losses, undue exposure and brand dilution long-term. Carries must also address these blatant network vulnerabilities and offer protection and contractual assurance against optical taps to their customers. Government must better protect their networks from all types of optical taps, proactively pursue and apprehend those who utilize such methods illegally, and help educate and empower organizations and citizens against such real threats. Those groups not willing to address and correct the issues surrounding optical tapping techniques will find themselves at a distinct competitive disadvantage long-term from a financial and risk exposure point-of-view.

REFERENCES

Alwayn, Virek. "The Physics behind fiber optics". *Fiber-Optic Technologies.* 23 April, 2004.

ARC Electronics. "Brief Over View of Fiber Optic Optic Cable Advantages Over Copper". *The basics of Fiber Optic Cable – A Tutorial*. Date unknown.

Book, Elizabeth. "Info-Tech Industry Targets Diverse Threats. Fears of network vulnerability fuel market for improved security systems". August 2002.

Corning Incorporated. "Basic Principles of Fiber Optics", *Corning Cable System*. Author Unknown. 2005.

Fiber Optic Association. "Understanding Fiber Optic Communications". 2004.

Goff, David R. "A Brief history of Fiber Optic Technology", *Fiber Optic Reference Guide,* 3rd ed. Focal Press: 2002.

LightSpeed MBPS, Inc. "Fiber Optics 101". Date unknown.

Oyster Optics, Inc. "Securing Fiber Optic Communications against Optical Tapping Methods", *White paper on optical taps and various solutions*. 2002-2003.

Poole, Craig D. "Optical fiber tap with integral reflecting surface and method of making same". *US Patent 6,535,671*. March 2003.

Snawerdt, Peter, "Phase-Modulated Fiber Optic Telecommunications System". *US Patent 6,469,816*. October 2002.

Svoboda, Elizabeth. "Code Breakers Stuped by Photon-Based System." *Discover,* January 2005. 33 vol. 26, No. 1

Tapanes, E. and Carroll, D. "Securing Fiber Optic Communication Links Against tapping", *Fiber Secure Link – White Paper.* Date unknown.

Walter, Herbert, "Method and device for extracting signals out of glass fiber" *US Patent 6,265,710.* July 2001.