OYSTER OPTICS, Inc.

Securing Fiber Optic Communications against Optical Tapping Methods

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 of 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 types 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 Oyster Optics' patented optical security, monitoring, intrusion detection and breach localization solutions.

INTRODUCTION

Fiber optic telecommunications systems make up the backbone of all modern communications networks. Whether voice, data, video, fax, wireless, email, 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 simple to tap, but in many respects they are simpler 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 communications in the fiber plant with little or no chance of detection.*

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 targets for attacks.

Traditionally illegal entry into systems has been through tapping 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 from undetected fiber optic taps that may remain in place for extended periods of time and provide access 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.

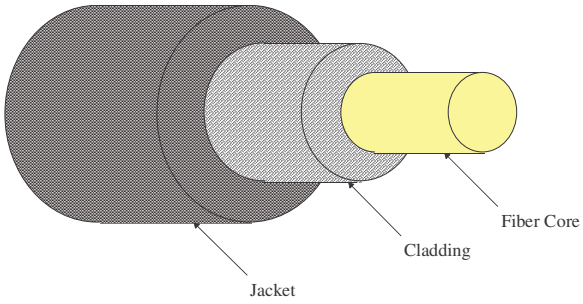
As a result, contrary to popular belief, fiber optic telecommunications systems are extremely vulnerable to being tapped and few private or public network operators, if any, can claim that their networks are 'tap free' or protected even minimally from optical tapping methods.

FIBER OPTIC COMMUNICATIONS

Optical fibers are dielectric wave guiding devices used to confine and guide 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.

Diagram 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.

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 thought 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.

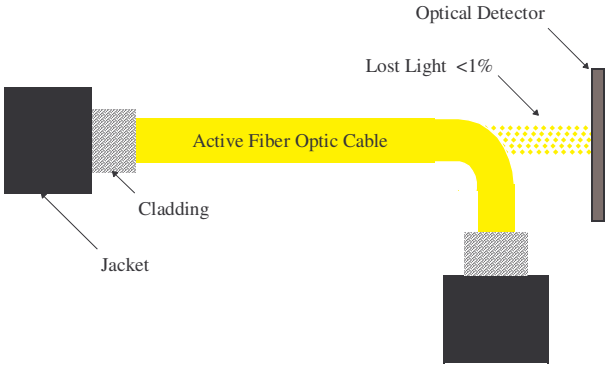
There are various fiber optic tapping methods, but most fall into the following main categories:

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

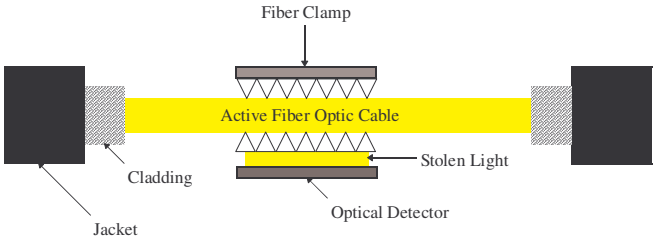
SPLICE: The simplest method of tapping is by splicing the optical fiber briefly and inserting equipment to allow for the signal to transit to the end party while also being intercepted by the intruder. Optical splices do provide a momentary lapse of data while the fiber is not operational. Carriers do 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.

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.

<u>Diagram 2:</u> Illustrated below are two simple taps that allow for the bleeding of light from the optical fiber.



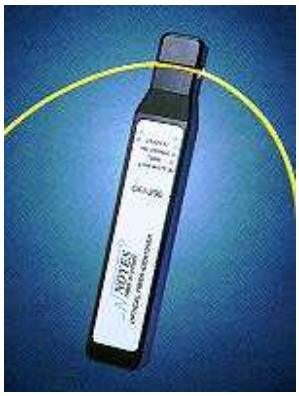
2(a)



2(b)

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.

Figure 3(a-d): Commercially available optical signal tapping device 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).



3(a)

3(b)

3(c)

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 signal. 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 communications.

NETWORK DISRUPTION: In fact, some tapping devices 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.

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 signals 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 plant 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.

3(e). Example of the tapping of a live video conference over a 10 kilometer fiber 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.

OTHER PARTIAL PROTECTION METHODS:

RFTS: Radio Frequency Testing Systems ("RFTS") are an effective means of scanning multiple dark fibers for route integrity prior to the optical fibers being lit. While certain types of discrepancies may be found, which could correlate to already placed taps, RFTS' only operate on dark fibers prior to service. Thus, once an RFTS is dismantled and a fiber is lit and in service, no form of even basic intrusion detection is left available. Furthermore, the optical signals on the lit fiber are in no way protected, so that an optical tap can readily extract data without the possibility of being detected. In short, an RFTS may provide some protection to optical network assets prior to going into service, but once in service and producing revenue, those assets are wide open to manipulation via optical taps.

Intrusion Detection Systems: Intrusion detection systems may operate on the data-layers or on the physical-layers. What most people understand as intrusion detection systems actually operate at the data-layers and offer no protection against optical taps. Intrusion detection systems that operate at the physical-layer are in fact useful in detecting if certain types of optical taps may have occurred. They do not, however, actually protect the underlying data at all, and thus such data may successfully still be extracted. Furthermore, intrusion detection systems are prone to human error, as alarms must be correctly interpreted and acted upon, otherwise unprotected data may continue to be tapped. In fact, non-touching optical tapping methods are by definition not detectable, and thus if the data itself is not protected, it may continue to be extracted indefinitely without any notice. Thus while physical-layer intrusion detection systems play an important role in fiber optic security in general, they serve more efficiently as part of a comprehensive security and monitoring package, which also incorporate other effective data and fiber protection mechanisms.

Encryption: While encryption is an effective means of scrambling data point-to-point on a network, it does not solve the problem of optical taps. Specifically, it does not protect the physical transport layer of the network, nor can it detect when an optical tap has been placed, what type of tap it might be and exactly where such a tap is located in the fiber plant. Without the ability to detect and locate a potential intruder, effective law enforcement actions are not possible. Therefore intruders are not only capable of continually and indefinitely extracting data in an undetected manner, but they are also in the position to insert further optical taps into other networks for additional gain in a relatively low-risk environment.

Encryption is also by definition a mathematically solvable algorithm with a predefined set and one correct key, which through various methods can be derived. So-called 'unbreakable' encryption methods have throughout history time and time again been broken with ingenious methods, faster processors, new technologies and simple brut force. Many decryption hardware and software tools for hackers are widely available and are quite successful at allowing unfettered access to data. Such examples include digital scanners for cell phones, DVD decoders, WiFi descramblers, and the like.

Encryption also has an associated high cost of ownership, as the difficulties in implementing and maintaining it across an entire enterprise are prohibitive. Usability is

also an issue as interoperability to other external organizations is not possible without proper planning and agreement on the types of encryption standards to attempt to use. As encryption is not a transparent security technology, users must learn various interfaces, which are not standardized across applications or platforms. Even then, encryption is only effective if keys are frequently updated and passwords are not simple to guess or find on or around workstation desktops. Large corporations with offices across the globe must also address various government export and import laws regarding encryption technologies, as well as government or 3rd party key depositories schemes.

Encryption has therefore experienced a relatively low implementation rate and virtually all voice traffic and the vast majority of data traffic is simply not encrypted today. The small amount of traffic that is encrypted, however, must have unencrypted headers in order to successfully transit and be switched in the public networks. Thus, traffic analysis can derive large volumes of useful data and encrypted packages between two parties actually serve as a red-flag for information that is potentially highly useful and may warrant the effort to decrypt offline.

Developments in quantum encryption have made headlines recently. It is important to note that while such efforts do protect the original encryption key when initially in transit, once a session is established, the actual information is sent in a normal encrypted format that is still susceptible to all the typical issues of encryption and likewise can be decrypted.

Therefore, while encryption may serve as a useful deterrent at the data-layer in general, a second complimentary line of defense at the physical-layer is required to truly protect against optical taps.

GOVERNMENT VS. COMMERCIAL NETWORKS

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 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.

PROTECTING INFORMATION

Based on the aforementioned evidence it is easy to conclude that by using relatively inexpensive opto-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, law firms, investment banks, brokerages, 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 optical 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 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 tapping is also less expensive and complex in the local and access loops, where speeds and network topology are simpler to manage.

In large cities and financial centers, optical network vulnerabilities are particularly magnified for systems in multi-story, multi-tenant buildings, such as high-rises, where users often occupy a number of non-adjacent floors. Optical cables linking the telecommunications facilities typically travel in risers or elevator shafts where there is no existing monitoring or security capabilities. Organizations 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.

LEGAL, REGULATORY AND INSURANCE IMPLICATIONS

Insurance policies are now widely available for various types of hacking, cracking and phreaking occurrences through firms such as AIG, Lloyd's of London, and Marsh. It is expected that insurance premiums for companies employing more secure services against optical taps will benefit from lower insurance premiums long-term.

Recent legislation has furthermore shifted increased security and privacy responsibilities to firms in both North America and Europe. Examples include: The Gramm-Leach-Bailey Act of 1999; The German Telecommunications Act (*TKG*) – Paragraph 87; The Health Insurance Portability & Accountability Act; The Electronic Signatures Act of 1998; The Child Online Protection Act of 2000; and The Internal Standards Organization (*ISO 17799*), to name a few.

In addition, other new laws such as the State of California's recent SB 1386 will require companies with online businesses to notify their customers of computer security breaches if they count Californians as customers, even if the company isn't based in California. Given the size of California's population and the complexity of differentiating between in- and out-of-state customers, many companies may be forced to inform all of their customers of computer security breaches in the U.S. and even abroad, when personal customer information is accessed or stolen.

Corporate Officers and Directors have also recently been held responsible for oversight of inadequate security measures in their own corporations. Various shareholder, contract, tort and insurance lawsuits have already been successfully litigated in court, or in many cases settled out of court, in order to reduce public exposure and risk brand damage. Examples include: People's Telephone Co. v. Hartford Fire Insurance; Exodus v. C.I. Host; Caremark Ash v. McColl; Oxford Health Plans; American Guarantee & Liability Co. v. Ingram Micro Inc.; International Derivative Litigation; Compare Retail Systems v. CAN Insurance.

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 exact 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. has 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 configurations for extremely secure government applications and networks are available. Oyster Optics also provides customized design, engineering and support services.

Corporate espionage of all sorts is 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 to the exact location where such instances 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 transmitter 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 provide further means of exploit through optical taps.

SERVICE PROVIDERS

Oyster Optics licenses its optical security, monitoring and intrusion detection technologies to communications equipment vendors and defense contractors for integration into their network platforms. Network operators can then purchase new equipment with Oyster Optics' technologies from such equipment vendors for insertion directly into their optical infrastructures. As optical security requirements become more stringent in the areas of physical-layer signal protection and intrusion detection, the demands within Service Level Agreements are expected to increase greatly, with customized escalation procedures for different types of intrusions becoming the norm. Long-term it is expected that corporations not utilizing secure optical bandwidth will be at a distinct disadvantage due to issues such as: greater network penetration exposure; higher insurance premiums; increased Officer and Director Liability; heightened brand risk; consumer backlash; negative press; etc.

Customers, however, may be offered a variety of service choices in the meantime. Oyster Optics' technologies are backwards compatible with existing telecommunications equipment and can run in either a secure mode or a non-secure mode. This distinct flexibility allows service providers using network equipment with Oyster Optics' technologies to offer their customers new pricing structures for secured data transmission, while still running in a non-secure mode for those customers not yet desiring extra security.

Oyster Optics provides three distinct advantages to carriers:

1. ***Differentiation:*** Oyster Optics enables carriers to provide truly secure optical networks to their corporate and government clients, who increasingly are looking for additional measures to safeguard their mission-critical data and communications across disparate global enterprises. Optical taps are a glaring hole in most companies'

security policies and effective protection tools are therefore needed for their security arsenal.

2. ***New Revenue Streams:*** Carriers implementing Oyster Optics secure transmission technologies are able to realize new revenue streams by providing secure bandwidth to their corporate and government clients directly to the premise. Carriers offering Managed Network Services can further revenue goals by implementing equipment with Oyster Optics' technologies as part of their core Network Security Solutions.

3. ***Cost Reductions:*** Oyster Optics' technologies help carriers achieve significant cost reductions through improved maintenance features, increased equipment performance and better resource allocation. Long-term cost savings may also be achieved through lower insurance premiums and reduced legal exposure.

OPTICAL NETWORK EQUIPMENT MANUFACTURERS

Changing optical security requirements over time will demand that manufacturers of optical networking equipment incorporate greater security, monitoring and intrusion detection functionalities into their platforms. Optical network equipment manufacturers meeting the needs of network operators benefit from three distinct advantages:

1. ***Platform Differentiation:*** Oyster Optics' technologies enable equipment manufacturers to provide truly secure optical networking equipment to network operators and thus differentiate their product offerings from that of their competitors. The threat of optical taps are causing network operators to consider the addition of optical security and monitoring features to their network platforms to protect their customers' confidential voice and data communications. Corporate end-users wishing to safeguard their mission-critical data and communications across disparate global enterprises are turning first to their network operators for solutions. Optical taps are a glaring hole in most platforms' security effectiveness and thus additional protection tools and policies are required.

2. ***Revenue Enhancement:*** Optical networking equipment manufacturers implementing Oyster Optics' secure transmission technologies are able to realize greater revenues by commanding a higher price for equipment providing such desirable security, monitoring and maintenance features.

3. ***New Market Penetration:*** No optical networking platform today adequately protects against optical taps, if at all. Networking equipment incorporating such security and monitoring capabilities may thus be used as a competitive advantage to successfully increase market share against competitors' product lines, which do not offer such functionality. Once in place, such security technologies may also be leveraged into higher-order equipment sales at higher margin.

SECURE OPTICAL PLATFORM: TWO INTEGRATION METHODS

Oyster Optics' proprietary technologies can be implemented into a manufacturer's equipment as either a stand-alone device or at the transceiver card level.

Stand-alone Device: When implemented as a stand-alone device, interoperability with any manufacturers' equipment is ensured.

The successful insertion into multi-vendor networks help protect network operators from financially troubled vendors and those not pursing optical security and monitoring functionality in their current or future product lines.

Such devices sit at either end of a given fiber optic segment to provide security, monitoring, intrusion detection and maintenance capabilities to that specific route. At either end, each device optically interfaces with already existing multiplexor and transceiver card equipment, which otherwise does not support such optical security and monitoring capabilities.

Network Management and Administration occurs through a standard SNMP or other similar interface. Multi-vendor interoperability in particular allows network operators to incrementally add such required optical security and monitoring capabilities to their already existing infrastructures. Network operators are thus not hampered by feature restrictions on current vendor equipment, limited configurations for security, network monitoring limitations or other constraints.

Transceiver Cards: When implemented at the transceiver card level, Oyster Optics' technology takes advantage of already existing optical and electrical components in the transceiver cards and their accompanying multiplexors or other terminal equipment. Transceiver cards are the least expensive, most easily swappable components in an optical network, and due to the life of laser components, need to be replaced more frequently than other networking equipment.

Thus network operators may replace existing non-secure transceiver cards in multiplexors and switches with secure transceiver cards containing Oyster Optics' technologies, either proactively in routes where need demands or through regular attrition. The cost differential between a current non-secure transceiver card and a secure transceiver card implementing Oyster Optics' technologies is the relatively minor incremental components cost, as well as other fixed costs such as upfront design and related licensing fees, which can be spread across the product line.

Even though the input and output electronic data streams to the multiplexors and switches remain the same, the light transmitting the data is in a patented secure phase modulated format different from any commercially available products. Because of the format of the light, Oyster Optics' technologies are therefore able to provide an extremely precise and sensitive tap detection system, which would not function with existing common equipment utilizing insecure amplitude or intensity modulated signals. Furthermore, Oyster Optics integrates an Optical Time Domain Reflectometer ("OTDR") to instantaneously locate the exact source of an intrusion or maintenance event and determine its origins, such as an actual tap, a physical line break, or even simple fiber degradation.

Such features also allow a carrier to more cost-effectively maintain and operate their fiber network. Depending on the type of breach event, the most appropriate resources may be allocated to alleviate the situation, whether it is a maintenance action or a law enforcement action driven by an actual intrusion.

Network operators may therefore offer corporate clients a much more robust and secure network, which is completely protected against optical taps and continuously monitored 24/7/365. Such

value-added security, monitoring and intrusion detection services demand a premium and would be a welcome addition to the current weak environment in the telecommunications industry.

Oyster Optics' technology thus manipulates the underlying characteristics of the light waves in such a manner, that when attempting to tap an optical fiber protected by Oyster Optics' technologies, it is virtually impossible to obtain information and to attempt to do so without the detection and localization of the intruder.

Oyster Optics' unique ensemble of security, monitoring, intrusion detection and breach localization technologies at the physical transport layer provides carriers, vendors and end-users with an unparalleled new security offering.

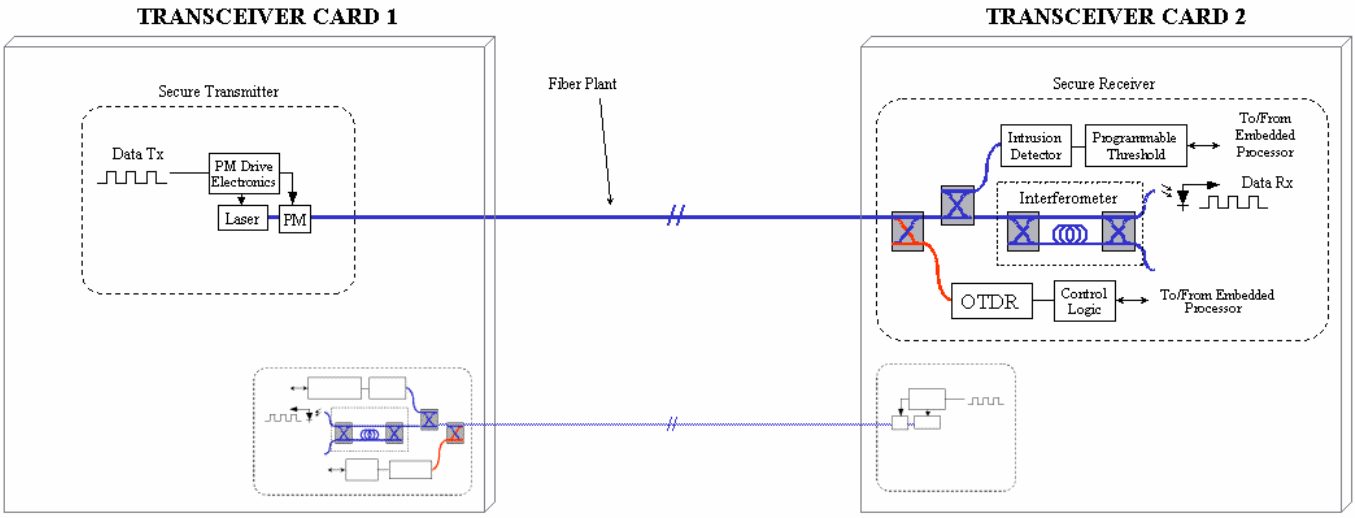


***Figure 4**: Example of Oyster Optics' Patented Secure Transmission Architecture*

Oyster Optics Transceiver Equipment Interfaces

For a transceiver card implementation to leverage the advantages of Oyster Optics' technology in a network, an upgrade to the existing embedded host platform software, network management software, and provisioning software should be implemented. The embedded host platform (i.e.: multiplexor, switch, or other equipment) and network management software upgrade consists of managing, controlling, and the automatic interpretation of the results from the intrusion detection alarm and embedded Optical Time Domain Reflectometer ("OTDR"). Network provisioning software upgrades will highlight routes that are protected by Oyster Optics technologies vs. unprotected routes, allowing carriers to optimize the rollout and support of new optical security and monitoring services in their networks. Nonetheless, because Oyster Optics' technology is backwards compatible with existing telecommunications equipment, it is possible for carriers to install and operate transceiver cards with Oyster Optics' technologies in a non-secure mode without requiring all necessary software updates to be in place. As a carrier's normally scheduled software upgrades occur, the new security, monitoring and intrusion detection services can be automatically 'turned-up' remotely to allow fast provisioning to corporate and government customers. Oyster Optics can also provide hardware and software support services during equipment design and integration with a carrier's selected equipment vendors.

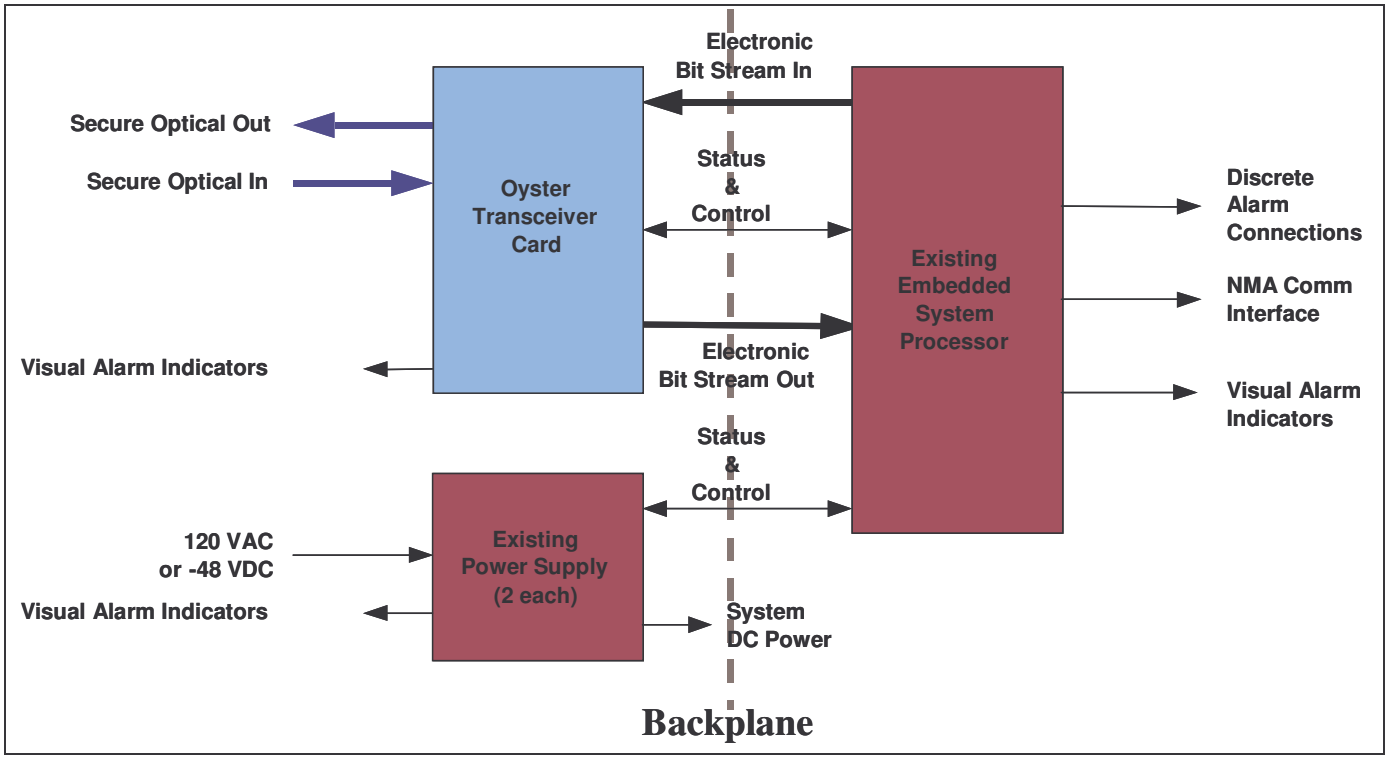


Figure 5: MUX/Terminal Equipment Interfaces for a transceiver card implementation

Optical Network Configurations with Oyster-enabled Products

Secure transceiver cards with Oyster Optics technologies can be implemented in all modern network architectures. Recent advancement such as all-optical switching, DWDM, integrated optical components and tunable lasers may also take advantage of Oyster Optics' patented technologies, which can be integrated into the relevant transceiver cards, modules, sub-systems, or stand-alone devices.

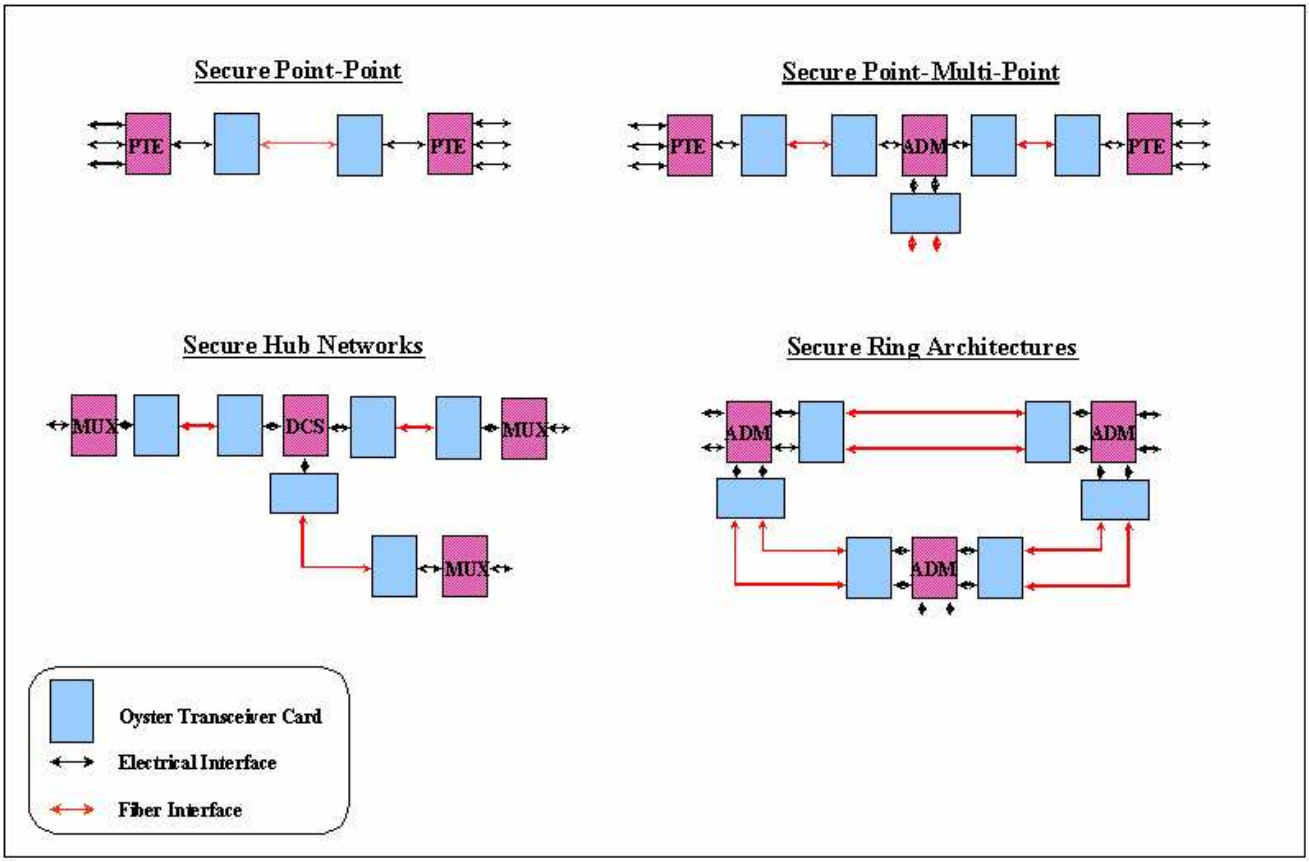


Figure 6: Optical Network Configurations with secure transceivers cards utilizing Oyster Optics' technologies

CONCLUSIONS

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 the 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 communications 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. Carriers must also address these blatant network vulnerabilities and offer protection and contractual assurances against optical taps to their customers. Governments 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.

Oyster Optics has a unique combination of security, monitoring, intrusion detection and maintenance technologies, which specifically combat optical taps. Oyster Optics' proprietary technologies completely secure the entire optical signal, making the extraction of data virtually impossible. Highly sensitive intrusion detection technologies monitor the optical fiber for network intrusions, identify the type of breach, and locate the position of the disturbance in the fiber plant in real-time, allowing the apprehension of intruders.

Output optimization technologies further greatly limit the available light a potential intruder would have at their disposal thus increasing their risk of discovery. As an integrated solution, Oyster Optics' secure technologies provide the greatest assurance of integrity, confidentiality and availability of the fiber plant available today.

Oyster Optics licenses its patented technologies to optical equipment manufacturers for inclusion in their platform at the transceiver card level or as a stand alone, vendor-independent device.

Key Features of Oyster Optics Technology

- Encryption-Free, Protocol-Independent Secure Data Transmission
  - ATM, IP, standard TDM
  - Fast Ethernet, FDDI, SONET/SDH, etc.
  - Voice, Video, Data, Imagery, etc.

- Compatible with all Modern Network Architectures
  - SONET/SDH Rings up to OC-192 (OC-768 in the near future)
  - WDM/DWDM Transport
  - Optically Switched Networks

- Bundled Security and Network Maintenance Features in a single package
  - Fiber Optic Cable Fault/Intrusion Detection & Location
  - In-service OTDR capability

- Seamless Network Integration - works with any manufacturers equipment

- Backwards-compatible with existing Network Hardware

To obtain additional information, please contact:

Oyster Optics, Inc.
853 Seventh Avenue, Suite 6E
New York, New York 10019
Tel: (+1) 646-436-2437
Fax: (+1) 413-895-8292
email: info@oysteroptics.com

References:

For up-to-date references refer to website: www.oysteroptics.com

Frankfurter Rundschau, "Glasfaser mit Durchblick", September 4th, 2002, Mr. Gabor Papp - (In German Language) – www.frankfurterrundschau.de

Frankfurter Allgemeine Zeitung, "Wie einfach Glasfasern angezapft werden können", March 13th, 2002, Mr. Heinz Stüwe - (In German Language) – www.faz.de

Die Welt, "Glasfaserkabel sind nicht abhörsicher", February 3, 2002, Mr. Gabor Papp - (In German Language), www.welt.de/daten/2002/03/09/0309ws319100.htx?

Süddeutsche Zeitung, "Die Ganze Wahrheit", April 6, 2000, Mr. Hubertus Knabe – (In German Language), www.sueddeutschezeitung.de

Overview of Optical Taps for *Network World Security Newsletter*, February 19, 2003, *Oyster Optics, Inc*. – www.oysteroptics.com

U.S. Patents 6,594,055- July 15th, 2003 - *Oyster Optics, Inc.*

U.S. Patents 6,469,816- October 22nd, 2002 - *Oyster Optics, Inc.*

U.S. Patents 6,476,952 – November 5th, 2002 - *Oyster Optics, Inc.*

U.S. Patent 6,265,710 – July 24, 2001 - *Deutsche Telekom AG*

European Patent 0 915 356 – September 9th, 1998 - *Deutsche Telekom AG*

Federal Bureau of Investigation and *Computer Security Institute,* "2002 Computer Crime and Security Survey", Volume VIII, Number 1, Spring 2002 – Mr. Richard Power – www.gocsi.gov