Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Free-Space Optics: A Viable, Secure Last-Mile Solution?

Free-Space Optics (FSO) is a fibreless, laser-driven technology that supports high bandwidth, with easy to install connections for the last-mile and campus environments. It has been in use by the United States military for a number of years primarily in naval ship-to-ship communications. Free-Space Optics systems are starting to gain acceptance in the private marketplace as a solution to replace expensive fiber optic based solutions. What is Free-Space Optics? How does it work? Is it secure? This paper will try to answ...

Copyright SANS Institute
Author Retains Full Rights

AD

Free-Space Optics: A Viable, Secure Last-Mile Solution?

Introduction

Free-Space Optics (FSO) is a fibreless, laser-driven technology that supports high bandwidth, with easy to install connections for the last-mile and campus environments. It has been in use by the United States military for a number of years primarily in naval ship-to-ship communications. Free-Space Optics systems are starting to gain acceptance in the private marketplace as a solution to replace expensive fiber optic based solutions.

What is Free-Space Optics?
How does it work?
Is it secure?

This paper will try to answer those questions and educate the security community about the technology and security ramifications as the demand for high-speed links increases. First let's take a look at the common methods currently used for making the last-mile connection and some of the issues associated with each method.

The Problem

Connecting a company's data and voice facilities to the carrier's (telephone companies') infrastructure is considered the "last-mile". The most common carriers are AT&T, MCI WorldCom, Sprint and the Regional Bell Operating Companies. Additionally, there are now hundreds, perhaps thousands of CLEC's (Competitive Local Exchange Carriers). The last-mile is the most difficult and expensive to complete. Current estimates suggest that approximately 95 percent of corporate buildings are within 1.5km of a telephone or Internet Service Provider's fiber-optic infrastructure. But few of these companies are implementing a high-speed data solution. Connecting the last-mile usually involves laying new fiber-optic or copper cable which can be cost prohibitive due to the cost of having to trench or dig under existing streets, sidewalks, lawns, buildings, etc. Most of these solutions also require a hefty monthly charge, often in the thousands of dollars or more. Security is for the most part non-existent on these connections and is dependent upon preventing physical access to the cabling.

Copper Based Solutions

Slower copper based solutions include 56kbps DDS and ISDN (Integrated Services Digital Network) circuits. ISDN is a popular redundant link solution, its maximum data rate is 128kbps and it is normally used as a dial up connection. The ISDN dial up connection is completed within a couple seconds and the customer pays a small monthly recurring fee for the line and then is charged for ISDN line usage only when the line is used. ISDN does support and use PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) authentication when connecting to the remote device but natively provides no data encryption. Higher speed copper based solutions are based on T-1 and T-3 circuits. A T-1 is composed of 24 channels; TDM (Time-Division Multiplexing) divides the channels so that each channel has a specific time slot. Each channel is either 56kbps or 64kbps with most implementations today

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

using 64kbps. A fractional T-1 is simply a T-1 with less than 24 channels being used. For instance a company could use four channels of a T-1 for a total data rate of 256kbps. It should be noted that these speeds are bits per second and not bytes per second. A full T-1 (using all 24 channels) provides for a maximum connection speed of 1.536Mbps. A T-3 consists of up to 28 T-1s with the total available data rate being 44.736Mbps. A T-1 or a T-3 is a very common way to connect companies to their remote offices, customers, suppliers, and the rest of the world.

Voice is also carried on T-1s with each channel having the ability to carry one voice conversation. This means that a full T-1 can handle 24 concurrent phone conversations. A T-1 can be divided by using specific channels for voice and specific channels for data traffic; a drop and insert CSU/DSU (Channel Service Unit/Data Service Unit) accomplishes this function. T-1s and T-3s can be very expensive, ranging in price from $300.00 a month for a fractional T-1 to $25,000 or more a month for a T-3. The price is dependent upon the distance from the company's physical location to the telephone company's POP (Point of Presence). Prices also vary widely between telephone companies.

T-1s and T-3s map directly to the first two layers of the OSI (Open Systems Interconnect) reference model. The data-link layer protocols normally used are HDLC (High-Level Data Link Control) and PPP (Point-to-Point Protocol). Both protocols are considered encapsulation protocols and provide little security and no data encryption. PPP does offer the ability for the connection to be authenticated by the use of PAP or CHAP and is generally used when connecting to an ISP. PAP is used to exchange usernames and passwords when the connection is made; it unfortunately sends all of this in clear text. CHAP is also used at startup; it uses a one-way hash function and can be configured to exchange the hashes at random intervals to verify the connection. Both PAP and CHAP have security flaws and are generally not used on many circuits. T-1 and T-3 security is based upon the fact that the lines are usually buried underground and can be difficult to physically access. T-1s and T-3s are terminated at the buildings demarc (demarcation point) quite often located in the building's basement. The T-1 or T-3 line is normally extended from the demarc to the server room where a CSU/DSU and a router are required to convert the HDLC or PPP encapsulated data to Ethernet, Fast Ethernet or whatever physical/data-link layer protocol is being used on the LAN. If an individual was able to gain physical access to the T-1 or T-3 copper cabling either at the phone company or the company's demark it would be simple to garner all traffic on the line using a device that detects the electromagnetic waves from the cabling. This would be undetectable from an Intrusion Detection System standpoint and would require physical security including secured locked equipment rooms and continual physical monitoring of cable runs for the presence of wire tapping devices.

DSL and Cable modems are also popular last mile solutions but are designed primarily for home users and not for businesses. There are exceptions to this such as a small remote office using a VPN (Virtual Private Network) connection over DSL to the central office. Some DSL providers have gone bankrupt and caused huge difficulties for companies dependent upon their DSL Internet connection. Another issue with some DSL

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

and Cable modems connections is that the providers will bridge a number of customers on the same broadcast domain causing security headaches. It's similar to everybody on your block being on your LAN. Use a firewall!

Fiber Optic Based Solutions

Larger corporations are using fiber optic connections to connect to their carriers. SONET (Synchronous Optical Network) is a set of standards used to define the rules required for interconnecting between companies and carriers. SONET also defines how to achieve redundancy by the use of SONET rings. For true redundancy, separate trenches must be used to prevent a backhoe or similar device from cutting both rings simultaneously. Speeds range from 10mbps to multiple gigabits per second.

There are two basic types of fiber cable, single mode and multimode fiber. Single mode fiber is composed of a single, thin strand of fiberglass or plastic and is used for long distance connections of up to 60 kilometers. Lasers are required to transmit the data on a single mode fiber connection. Multimode fiber is composed of a slightly larger diameter single strand of fiberglass or plastic and is used for shorter connections of up to 2 kilometers. Multimode fiber connections normally use a LED (Light Emitting Diode) for the transmission of data. Multimode fiber optic cable maximum distances are shorter than single mode because the light pulse can take separate paths through the cable. As the cable distance increases the light pulses which bounce around the cable can arrive at the receiver at different times making the signal unreliable. Multimode fiber uses less expensive equipment to process the light pulses and is used more often than single mode unless the distance is too great. A fiber optic connection requires a pair of fiber optic cables, providing full duplex operation. T-1s and T-3s are mapped directly on to the SONET fiber optic solutions providing both voice and data connectivity. Installations of fiber optic connections can take anywhere from one month to a year or more because of the permits required to excavate the trenches.

Fiber Optic connections are considered very secure. Data is transmitted as beams of light so no electromagnetic waves are generated. Insulation surrounds the fiber optic strands making it impossible to detect the light pulses without tapping into the actual strands. The fiber strands are extremely thin and virtually impossible to tap into without breaking the strand, which would immediately shutdown the connection.

Wireless Connections

The opposite of a secure, private, fiber optic cable solution is wireless. By default wireless solutions broadcast data to everyone within range. WEP (Wired Equivalent Protocol) tries to provide some security but has a number of flaws. The SANS reading room has a number of good articles on wireless security if more information is required.

Free-Space Optics

Most of the technologies discussed so far are WAN (Wide Area Network) based. Free-Space Optics (FSO) is a technology similar to fiber optic cable infrastructure except that no cable is involved. The light pulses are transmitted through the atmosphere in a small conical shaped beam by the means of low powered lasers or LED's. The technology has

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

been in existence for over 30 years and is now available from a number of vendors. Free-Space Optic installations require line-of-sight availability between the laser/receiver units which are called link heads. A thorough pre-installation site evaluation must be done to ensure that the paths between the Free-Space Optic units are clear and will remain so for a number of years. The growth of trees and the construction of buildings need to be considered along with any aesthetic issues and required permits. The units can be mounted on building tops, sides and even behind windows. Speeds range from single T-1 and 10Mbps to 2.5Gbps on currently available products. 40Gbps has been successfully tested in laboratories; speeds could potentially be able to reach into the Terabit range. The units are full-duplex meaning that data can flow in both directions simultaneously. The lasers are low power and do not constitute a risk to the naked eye or any bird or animal that might get in the laser's path. The various vendors offer multiple ways to connect the Free-Space Optics equipment to the LAN or WAN equipment including standard fiber based optical connectors, 10BaseT, 100BaseT, 1000BaseT and other connectors. The frequencies used by the lasers are between 750 and 1550 GHz and do not require special licensing like other wireless devices.

With the advent of VOIP (Voice Over IP), videoconferencing and streaming, new high bandwidth applications, etc., bandwidth requirements for all aspects of the network are constantly increasing. The legacy WAN technology described earlier in this paper is not a technology suited for the evolving MAN (Metropolitan Area Network). There is no need to use the dated T-1/T-3 technology to separate voice and data. Voice becomes another application on the network using IP data packets to route and provide phone services. MAN environments are basically a continuation of the LAN (Local Area Network) to include resources based not on a single building but on a small geographic location. A college campus would be an example of a MAN, where all of the college's buildings have high speed Ethernet links between the buildings. Most MAN's are based on a 100Mbps or higher Ethernet backbone. Fiber optics is the preferred technology for interconnecting the MAN because of the maximum lengths available and the bandwidth potential. But fiber can be expensive to install and the monthly recurring fees can also be very high. Free-Space Optics can be used to augment or replace fiber based MAN solutions. The different vendors of Free-Space Optic systems provide products that operate in just the physical, the physical/data link, and the physical/data link/network layers of the OSI reference model. This allows virtually any protocol that runs on fiber based installations to also run on Free-Space Optic systems, including the ability to map T-1s onto the link. The systems including network layer operability also use routers to segment the Free-Space Optic links. Many solutions incorporate a partial mesh design so that if one link fails for any reason, a redundant path is almost immediately available. In reviewing the impact on networks from the disaster on 9/11/01 many corporations are considering decentralizing data processing centers. This will also contribute to the growth of high bandwidth MANs.

One of the main issues with the technology is that fog and severe weather can have a detrimental impact on the performance of the Free-Space Optic systems. The main factor is fog, with rain and snow also contributing to the maximum distances that can be

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

achieved. The following table is taken from a white paper on the Optical Access web site and is representative of the impact of fog and bad weather on the operational distance of a Free-Space Optic system.

Weather condition	Precipitation	mm/hr	Visibility	dB loss/ km	TerraLink 8-155 Range
Dense fog			0 m		
			50 m	-315.0	140 m
Thick fog			200 m	-75.3	460 m
Moderate fog			500 m	-28.9	980 m
Light fog	Cloudburst	100	770 m	-18.3	1.38 km
			1 km	-13.8	1.68 km
Thin fog	Heavy rain	25	1.9 km	-6.9	2.39 km
			2 km	-6.6	2.79 km
Haze	Medium rain	12.5	2.8 km	-4.6	3.50 km
			4 km	-3.1	4.38 km
Light Haze	Light rain	2.5	5.9 km	-2.0	5.44 km
			10 km	-1.1	6.89 km
Clear	Drizzle	0.25	18.1 km	-0.6	8.00 km
			20 km	-0.54	8.22 km
Very Clear			23 km	-0.47	8.33 km
			50 km	-0.19	9.15 km

Snow

Isaac I. Kim, Ron Steiger, Joseph A. Koontz, Carter Moursund, Micah Barclay, Prasanna Adhikari, John Schuster, Eric Korevaar "Wireless optical transmission of Fast Ethernet, FDDI, ATM, and ESCON protocol data using the TerraLink laser communication system."
http://www.opticalaccess.com/documents/lasercom.pdf

Vendors have created tables that list the average yearly fog levels for most of the major cities. When planning a Free-Space Optic system, it is recommended that someone review the city's fog table and the anticipated distance of the connection. The vendor's product specifications should be used to ensure that the product will perform in a satisfactory manner for the connection. Other factors involved in limiting the distance of the connections is the atmosphere itself. As the beam goes through small pockets of differing variations in air temperature and wind speed the light can be refracted off course. Since these variations are physically very small, most vendors will use multiple lasers in parallel on the Free-Space Optic system to compensate, especially on units designed for longer distances. Since RF (radio frequency) wireless systems like the ones based on the 802.11b standard are not affected so much by fog, some manufacturers are using these as a redundant system and have incorporated them into their Free-Space Optic systems.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Free-Space Optics can be an important component in a corporation's disaster recovery plan. The links can normally be installed within four hours or less with the company not being dependent on having to wait weeks or possibly months for a carrier to install the copper or fiber based circuits.

Free-Space Optic Security

Even though Free-Space Optics is a wireless technology it does not have the nasty habit of broadcasting to anybody and everybody. It instead transmits a very high frequency narrow beam of light to a specific destination. In order for an individual to intercept the beamed signal they would somehow have to wiretap the beam. Actually, there is no wire so the word wiretap would not be correct. Hmm, since this is a new technology we're dealing with, let's invent a new word. For the purpose of this paper we shall use the words or terms beamtap and beamtapping to describe the process or equipment used in trying to garner data from a beam of light transmitted by a Free-Space Optic system. As this technology is quite new to the marketplace, little information was found on the security of Free-Space Optics. The three following quotes were taken directly from the vendors' web sites.

"To ensure high security, Terabeam's optical stream is directional and limited to a small diameter, so only Terabeam's site equipment can receive data sent from the Terabeam network."
http://www.terabeam.com/our/our_gen.com

"Optical link is directional and limited to a small diameter only optical link can receive data."
http://www.furtera.com/fsofaq.html

"In addition, because the OPTera Metro 2400 is laser-based, it is much more secure than other wireless solutions—its narrow laser beam is not accessible unless viewed directly on the transmission path. Therefore, it is virtually impossible to intercept its signal without being detected."
http://www.nortelnetworks.com/products/library/collateral/56328.02-06-01.pdf

The vendors have a good position. Free-Space Optics is far superior to an 802.11b wireless system broadcasting data everywhere, but a couple scenarios need to be addressed. It would be difficult for an individual to beamtap without physically exposing himself and his equipment. The Free-Space Optic systems are normally installed as high as possible so that passing cars, trucks or other moving things do not interfere with the beam. A bird can disrupt communication but it is only momentary and the system will very quickly recover. By contrast, beamtapping would require that a mirror or other device remain in the beam path for extended periods of time. Care would need to be taken by the intruder to not disrupt either beam because if one beam is interrupted the other beam would automatically go into failure recovery mode and would not transmit any data of interest to the intruder.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

It was mentioned earlier that the Free-Space Optics systems transmit a conical shaped beam of light with the beam expanding more and more as it leaves the laser and goes through the atmosphere. The conical shapes differ from one another in size; some designs send a very narrow beam and other designs send a wider beam. The reason for this difference is the fact that tall buildings will sway back and forth due to strong winds and earthquakes. Since the systems are usually installed at the top of buildings the units can move in and out of the beam of light when the building sways, losing synchronization with one another. The Free-Space Optics vendors address this issue in one of two ways. One way is to keep the beam narrow and use a system that automatically aligns the equipment, keeping them synchronized to each other when the buildings move. The other way is to simply make the conical beam widen quicker, making the beam wide enough at the far end so that even if there was building movement the units would remain in each other's beam. It is much simpler and cheaper to design a Free-Space Optic system with a wider beam than to make one that automatically stays aligned. Both types of systems are available from vendors. At a distance of one kilometer from the laser, the diameter of the beam is about one meter on a self aligning system and can be three to six meters on a non-self aligning system.

Beam size is important to securing the connection. The larger the beam, the easier it would be for someone to find the beam and to place a mirror or receiver in the beam and not disrupt either connection. If an individual wanted transmitted data from both ends of the connection simultaneously, the beamtapping device would need to be placed approximately equidistant between the Free-Space Optic units. The closer the beamtapping device is placed toward one end or the other, one of the conical shaped beams would become smaller and the likelihood of disrupting the beam would be greatly increased thus stopping the connection. Admittedly, placing a beamtapping device between Free-Space Optic units would be difficult to do in most circumstances. The beam is very small, would be difficult to locate and is generally very high and not close to anything. The chance of being discovered is real, because by blocking one of the beams, the company when investigating the problem could discover the intrusion attempt. Since the beam needs to be line of sight, surveillance cameras could easily be used to monitor the installation and beam path to detect any suspicious activity.

A greater concern is the beam extending past the Free-Space Optic equipment for a few kilometers. The Free-Space Optic equipment takes around a square foot or less of the beam, so in most scenarios the majority of the beam extends past the intended target. Only one side of the data conversation could be beamtapped in this case, but that could easily be the part of the data stream of interest to the individual. The beamtapping would probably never be detected and could continue for years. The solution here is to determine the size of the beam at the receiving point by using the distance of the connection and the vendor specific beam dispersion formula. Once the diameter of the beam is determined plan the installation so that the Free-Space Optic equipment has a wall or similar nonreflective surface directly behind it to block the remaining remnants of the beam. A wall could be built to block the beam if required. Physically monitoring the installation would be recommended to ensure that a beamtapping device was not mounted on the wall or somewhere near the Free-Space Optic equipment.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Encryption equipment could also be used on each end to encrypt and decrypt data. It would be very difficult to find encryption devices that could support the speeds that Free-Space Optics are capable of, but it is an alternative. In doing research for this paper an interesting technology was discovered that is currently under development. It involves applying a varying analog input to a laser and the laser responding by transmitting a digital chaotic output. The theory is that if the receiving end had a similar analog input the chaotic signal could be decrypted. Any device intercepting the signal would view it as being chaotic and could not discern a pattern or be able to crack an encryption algorithm. This technology could potentially be used on Free-Space Optic equipment making encrypted high-speed connections a reality.

Conclusion

The future will require higher and higher bandwidth solutions to meet the needs of corporations and individuals. Cost effective alternatives need to be found to augment the legacy WAN technologies in providing secure, redundant links between corporate resources, the Internet and the telephone company carriers. Free-Space Optics can meet these needs and will be used in an ever-increasing way to provide these solutions in the future.

References:

Heinz A. Willebrand, Baksheesh S. Ghuman "Fiber Optics Without Fiber."
http://www.freespaceoptic.com/Fiber_Optics_Without_Fiber.htm

Roosevelt Giles, "CCIE Study Guide" McGraw Hill, 1999

http://www.bandwidthplace.com/service.html?service=oc&page=1

http://www.bandwidthplace.com/service.html?service=oc&page=2

Gregory A. McGill "Elements of Wireless Security
http://www.sans.org/infosecFAQ/wireless/wireless_sec2.htm

Rolf McCellan & Jim Metzler "Designing the new MAN" Network World, 11/05/01

Isaac I. Kim, Ron Steiger, Joseph A. Koontz, Carter Moursund, Micah Barclay, Prasanna Adhikari, John Schuster, Eric Korevaar "Wireless optical transmission of Fast Ethernet, FDDI, ATM, and ESCON protocol data using the TerraLink laser communication system."
http://www.opticalaccess.com/documents/lasercom.pdf

"Using Chaos For Secure Communications: Using Chaotic Lasers For Encrypting Sensitive Data"
http://www.globaltechnoscan.com/28feb-5march/secure.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Valerio Annovazzi-Lodi, Silvano Donati, Alessandro Scire "Synchronization of Chaotic Lasers by Optical Feedback for Crytpographic Applications."
http://ele.unipv.it/~donati/papers/49d.pdf

© SANS Institute 2002, Author retains full rights

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**