International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Securing Fiber Optic Networks and Designed According to the Security Standards

Algasim Mohamed Ahmed Abd Albagi[1], Dr. Amin Babiker A/Nabi Mustafa[2]

Department of telecommunication, Faculty of Engineering, Al Neelain University, Khartoum, Sudan, 2014

Abstract: ***This paper contains a description of optical fibers networks which characterized by high immunity of penetration and a review of the most important techniques of optical fiber penetration and presentation the best mechanisms to detect breaches and the most effective ways to identify security risks in the optical networks and a description of the techniques of intrusion detection and network monitoring, which provides detect and locate breached fiber in the optical network.***

Keywords: penetrate, taps, prevention, OTDR

1. Introduction

Despite the fact that fiber optic cables are characterized by high resistance to interception (interception) and taping ((taping at least if what has been compared with cables but scientifically proven the possibility of success intercept the optical signal in many accidents in the world, especially when it is responsible for the network security on non-fully aware of the areas and situations weakness and danger in the network, as well as when the mechanics of intrusion prevention and intrusion detection mechanisms contained and is activated in the network management practices. For the purpose of covering all the paragraphs that relate to security optical network it there are multiple ways to break through the optical fiber (fiber taping), including common way by bending or foldable optical fiber (fiber bending), and by separating or splitting, and networking or evanescent coupling, and the scattering or dispersion, the way to do an incision (gully) in the form of symbols V (v-grooves) in the optical fiber. This taping ways are characterized by it require to use a complex and difficult devices to be able to change the physical properties of the fiber optic in the field , with there is a high probability of risks to destroy or break for fiber optic leading to detect attempt penetrate the fiber by the end user. This study it will also touch on the optical signal losses which generated by bending the fiber (bend losses) and that lead to successful taping for the signal which transmitted in single mode fiber as well as the analysis of the characteristics of bending that can be used to detect whether there is a breakthrough process by bending the fiber.

These techniques include: The use of optical amplifiers and specifically which characterized by detecting tampering or intrusion devices (embedded tampers), Also the process of securing optical networks require the use of devices to measure reflectance optical with optical time domain to locate the occurrence of intrusions, Here will be the review of detection techniques and monitoring in this study, with a focus on the amount of the effectiveness and efficiency of each technique.

2. The most important mechanisms to penetrate optical fiber and optical networks

Despite the fact that the fiber optic cable with the highest security when compared to copper cables, but the process remains impenetrable as possible through access to its signal transmitted in the optical core. That all kinds of optical penetration include (signal interception) and access to the fiber optical cable inside. For the purpose of access to different ways of optical signals interceptions, it is necessary to recall how quickly the installation of optical cable. Optical fiber consists of two regions, which is the heart or inner (core) and external cladding or a casing (cladding) ,core of the optical fiber is the carrier of light from one of the ends of the network to the other end either casing (cladding) who shall to protect the core of the fiber, as well as works as a layer marginal along the outer edge of the core, which allows the light to be reflected entirely into core ,which leads to missing very few in the ability of signal ,that mean limit attenuation of the transition optical signal to long-distance and achieving the so-called principle of total internal reflection which is the basis in the light transmission process. For the purpose of to penetrate or intercept a signal light, it must to penetrate the core. For the purpose of access to the fiber, the penetrator must be up to the cable terminated end, where the fibers are bare which called (Red Equipment Area) or (gain - mid -span access to the cable). Despite the fact that access to the terminated ends of the fiber is preferred but this region have a high degree of security. so that the penetrator to achieve access through the area connecting the cable with another cable (mid-span-access), the penetrator must cut at least 12-24 inch from the outer casing (cladding) to access to the bare fiber in the center of the cable. When achieving the access the penetrator became have a several options for intercept or networking (tap) on the original signal.

The most important of these options or ways of penetration include the following:

1) Fiber bending
2) Optical splitting
3) Evanescent coupling
4) V-groove cut

2.1 Fiber Bending Way

Taping by this method is easier to use in the field. This method involves splitting a single fiber or scrape down to the cladding and bend the optical fiber, part of the optical signal leaves the optical fiber to the outside. The power of tapped signal will depend on the diameter and the angle of

bending. Optical detectors are used for increasing the capacity of the tapped signal whatever its small, So that the penetrator target will be using a minimum of losses in the fiber optic signal without completely objection or destroy optical fiber. So that this method can't be detect without continuous monitoring, tests and examinations on the web.

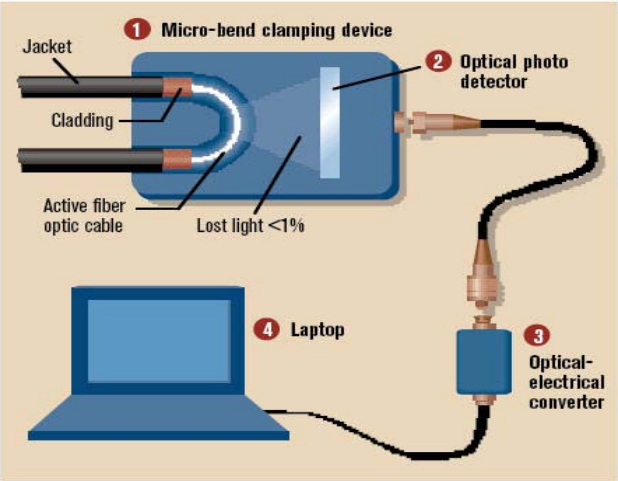

Figure 1: Optical bending way

2.2. Optical Splitting

Optical splitter split optical signal into two signals identical (Note :. can use a bottle or mirror partially painted and placed at an angle to steal little part of the beams carrying the information and allow the most part pass through the fiber). For the purpose of installing penetration technique the goal fiber must be cut and both ends must be spliced to each other on the optical splitter. In the case of access to fiber in the optic cable, the process of splicing optical fiber to the optical splitter may take 2-3 minutes depending on the method of splicing.

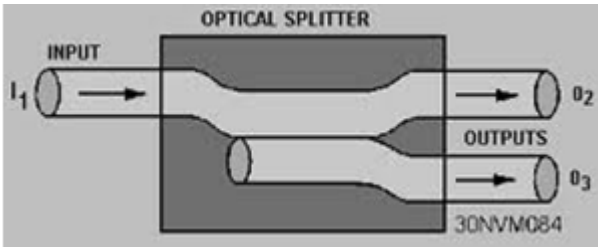

Figure 2: Optical splitter

2.3. Evanescent Coupling

In a similar fashion to the way the light beam splitter aforementioned, this method uses the same previous method, but without the need to slit the target fiber .it can build an optical splitter instead of using device tentatively made outside the optical cable through polishing the cover (cladding) and allow to a part of the light signal to be pick up through the tap fiber. Although this method look like featuring many of the beauties of the penetrative if what has comparable with the optical splitter method (because there is no tapping for the light beam and no mirror to split the light), but it is very difficult to apply this method in the field as well as it cause optical losses limits of 1-2 decibel. Optical fiber is smaller than 1/8 of diameter of a human hair, making it almost impossible to achieve the required accuracy in the field without the use of high-tech equipment and cumbersome to use and the subsequent long time to complete the process of penetration.

2.4. V-Groove Cut

In this method makes (gully) shaped v in the cladding of optical fiber and close to the heart of the fiber (core). The method of groove-shaped v the angle between the spread of the signal in the fiber and face groove must be greater than the critical angle for total internal reflection. If what has been achieved this condition, the part of the signal during the (cladding) and overlapped with groove-shaped v will suffer internal reflection and will coupled to the outside through the side of the fiber. Again, this method requires high precision cutting in the fiber as the consequent cutting of anti-aliasing or polishing requires high precision equipment and long time to install like this tapping. However, this method will cause a few losses in the light beam inside the optical fiber and thus be difficult to detect this type of breach. Finally, this is the most dangerous way to achieve a breach of the fiber optic field.

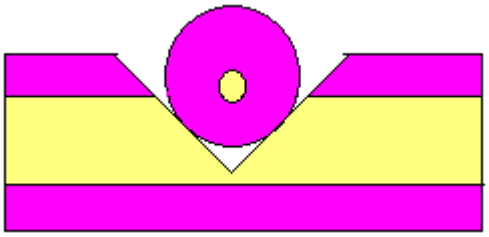

Figure 3: V-groove way

3. Detect breaches of the optical network: The devices which detect breaches

Through our review of the methods of penetration, it is possible to use one or more of these methods to penetrate a safe optical communications network. It's easy to use architectural networks and infrastructure and operations and ways to prevent or detect such breaches. That all methods of penetration of the fiber optic outlined previously will cause a change can be measured or detected using standard measure optic equipment, such as the use of optical test kit which measures the attenuation of optical (dB) as well as a optical time-domain reflectometer (OTDR) which measures the events or cases of reflection and non-reflection in a optical fiber circle.

3.1. Optical Tester

These devices depend on measurement of the amount of attenuation (the amount of loss in the optical signal) (dB) in the network. These devices consist of Light Source, which generates a certain amount of optical signal with different wavelengths and also consists of a measure of the power which is subject to calibrate for the purpose of accurate measurement of the received optical signal.

By knowing the amount of inserted optical signal to the network and find the amount optical signal received at the other end, it is possible to know the amount of losses in the optical segment. By recording the readings of attenuation for each fiber individually and which is tested over time, it is possible to trace the network degradation and to identify any discrepancies, which is considered an indication that the network had been infiltrated and he's got fiber taps.

3.2. Optical Time Domain Retlectometer (OTDR)

The idea of the Device (OTDR) is quite similar to the working principle of the radar in terms of that it is sending very precise pulses and measured multiple light wavelengths and then calculates the amount of time it takes to receive the returned signal again when the sender, as well as calculating the amount of optical intensity for this the returned signal. By tracking both the time spent and the intensity of the signal returning to the OTDR, the OTDR will be able to track the impact of the overall length of the circle of light and show all points of splices, connecters as well as the potential intercepts in the trace window. There is a major function for the OTDR which it determine the distance to any break in the cable or penetrate through testing and storage of spectral shape generated in the OTDR device, the end users have the ability to monitor changes in network circles and identify any potential optical intercepts.

4. Testing Effectiveness vs. Fiber Taps

Due to the fact that both of the optical test set and OTDR device differ in efficiency and complete the task of security screenings, the both have varying degrees of effectiveness in detecting and preventing breaches of light (optical intercepts). The optical tester device is able to achieve the potential of detecting relatively good for the fiber taping ways which became easy-implementation on the ground, but this method be weak to detect the most advanced fiber penetrate ways. But the OTDR achieves strong to moderate possibilities of detection across the network, and that because of the ability of the OTDR to determine the identity (detection) optical losses points which could be due to the penetration (tap) along the line of fiber. The optical tester device is able to achieve the potential of detecting relatively good for the fiber taping ways which became easy-implementation on the ground, but this method be weak to detect the most advanced fiber penetrate ways. But the OTDR achieves strong to moderate possibilities of detection across the network and that because of the ability of the OTDR to determine the identity (detection) optical losses points which could be due to the penetration (tap) along the line of fiber.

5. Network Integration of Detection & Prevention Capabilities

Network should include various optical test equipment, there are two types of tests and network monitoring (testing & monitoring), a passive testing and self monitor (automated monitoring)

5.1 Passive Testing

This test is the most expensive for the purpose of documenting and checking and monitoring and securing networks in order to determine whether there is decay or weakness in the service and the possibility of the occurrence of security optical intercepts. This type of tests Performing using stand-alone OTDR device or with the use of optical test set for the purpose of conducting periodic surveys, because the fact that this test is carried out at every part of the network equipment individually, it represents the most expensive way of protection with different degrees of transparency in the work of the networks. This type of test is also considered one of the tests that parasitize or intrusion the work of the network because it require to disconnected every circuit in the network from the switch to the complete of the examination process.

5.2 Automated Monitoring

For the purpose of achieving self-monitoring for the network, it is possible to integrate testing equipments directly in the network architecture and combined with optical switch in order to allow connect an optical test set to multiple optical circuits in the system. Because of the increased need for equipments and the need for optical switch the method of self-monitoring are expensive price but are considered the only way that can achieve self-monitoring for efficient performance of the network and signaling any attempt of optical penetrations or networking on the optical fiber.

6. Securing Optical Networks

6.1 Environmental Precautions

Environmental precautions must working on to take action fire prevention and protection from them, take action to prevent the risk of water, Protection of electrical power processors, control of moisture, take action protection from natural disasters such as earthquakes, lightning, thunderbolts, protection against magnetic fields, protection against dust and sand dunes.

6.2 Maintenance of Equipment in Order to Achieve Safety and Security Optical Networks

All the equipments for the network must be linked with the backup power supplies, Each network equipment must be locked in a closed cabin and keys with maintenance crew only, access to the closets and equipment racks should be allowed only to Network infrastructure operation group, Put surveillance cameras in all the network closets, In the case of the replacement of workers must replace the network closets, use quantum cryptography and phase modulation to protect the information optical fiber, use OTDR and optical tester to detect penetration.

6.3 Securing Fiber Optic Cable Paths

These is done by hide or bury the optic cable in concrete and use of armored cables, using continuous, real-time

monitoring, diagnosis of an anomaly in the optical signal, using automatic intrusion shutdown in network in the case of risk, adopt the principle of changing the path of carrier to the path of an alternative optical fiber at risk situations.

7. Conclusion

Although the fiber-optic be of very high degree of security compared to copper cables, it is still there ways in which hackers can of networking (tap) and intercept high confidential information transmitted via the optical network. The vast majority of ways to penetrate the fiber optic require a certain degree of access to or influence to the heart of the optical fiber. Regardless of the method used, the penetration can detect using test equipments such as optical device (OTDR) or optical testing set (OTS). Also process of detecting fiber taps can enhance its efficiency using ribbon cables instead of the loose-type or tight-buffered cables. According to the threat level or the degree of protection required, the network monitoring and testing can be done by passive way which use one of the stand-alone test equipments or by using the method of automated test. Regardless of the method used, the network monitoring must be as part of an integrated network management for the purpose of preventing and detecting optical breaches (intercepts) before they cause the disclosure of information related to national security or the security of the industrial institution, commercial or other.

References

[1] Yas Al-Hadithi, International School on Quantum Electronics, Free Space Optical Communications, Erice, Italy July 2007.
[2] Symantec Data Loss Prevention, Information Security and Employee Communication, Best Practices, 2009 Symantec, Inc... DATE 2/28/09 VERSION 1
[3] Kartalopoulos, S.V.; Communications, 2009. ICC '09. IEEE International Conference on 14-18 June 2009
[4] W. Alexander, D. L. Clark, and C .A. Stewart, Optical Engineering, Vol . 27, No. I, P. 14 , (1988)
[5] Investigating the possibility of building a free space optical communication system in Yemen, Submitted to the SPIE conference in Sweden Sept.2006.
[6] K. F. Hulme el., A CO2 laser range finder using heterodyne detection and chirp Pulse Compression, Optics and Quantum Electronics, Vol . 13, No. 1, P. 35, (1981) .
[7] Optical depth calculations of some spectral lines produced using KrF laser, J of Science and Technology, University of Technology, Baghdad, Iraq, P167-171, volume 19, no.2, 2000.
[8] P. K. Henry et al., Hg Cd Te Photodiodes for heterodyne application, Proc . SPIE, Laser Radar Te Photodiodes for heterodyne, Vol . 663, P. 142 , (1986)
[9] Numerical, Analytical and experimental study of optical fiber communication system security, International conference on information technology and National security, Saudi Arabia, Riyadh, 1 Dec - 4 Dec 2007.