Fiber optic is reliable with networking. i mean” how is it been secure”

Fiber Optics: A Better Alternative? Fiber optics has highly improved the way we humans communicate since the U. S. military first used it in the 70s. In fact, with millions of fiber optic cables stretching worldwide, it has been the backbone of the Internet and telecommunications systems.

Fiber optics is a technology that uses very thin transparent silica glass or plastic fibers to transmit infrared signals. These infrared signals, also referred to as light signals, can easily transmit sound, electrical, and even computer data. Amazingly, just one of these fibers can hold hundreds of various signals and transmit data at lights speed at the same time.

In a relatively short amount of time, a vast number of households and companies shifting from cable wires to this technological option. So just what makes this piece of technology so indispensable today?

In a study from the Sans Institute Reading Room site, it says that fiber optic cables " can go an average of 62 miles versus 1. 2 miles that copper can go before the signal needs to be regenerated or boosted." (Witcher, “ Option 1…”) Fiber optic cables also do not conduct electricity, since they are not metallic, which makes them less interfered by radio frequencies, electromagnetic interferences, or even lightning. They are also smaller and lighter than copper wires, and are not affected by atmospheric conditions making them even more " installation-friendly" to areas that copper wires cannot go. With all these, plus the fact that fiber optic cables do not produce electrical radiation, fiber optics has been the choice solution for a better and a more secure means of communication by companies across the globe.

However, it is not all good news.

Through the years, research has proven that fiber optic cables can be easily tapped. One, which is the easiest, is called splicing. Splicing is done by an

inserted apparatus intercepting a signal while it is currently transmitting data to an end party. However, this method is easily detectable by most network security systems. Another method of getting data from fiber optic cables is through splitters and couplers. This method is done by slightly bending, crooking or putting a clamp on an optical fibers length so that light photons will leak into the tappers receiving device. Lastly, there are the non-touch methods. The more advanced of these methods are able to derive the underlying optical signal by understanding the interactions between the fiber plant and the extra light added into it. Without any physical-layer optical signal protection, these methods are virtually undetectable.

Though threats arose, technology gave birth to partial protective methods to defend fiber optics from security problems. The first of which is the Radio Frequency Testing Systems or the RFTS, which checks multiple dark fibers for route integrity before they are lit. Next is the Intrusion Detection Systems (IDS), which operates on the physical-layers of the fiber optic cables. This particular system can detect certain types of optical taps that may have occurred. Encryption is another method of fiber optic security. With the use of strong encryption with long codes, information may be kept secure from hackers.

In conclusion, fiber optics is a better alternative than copper wires. And with the years to come, fiber optics will continue to do wonders for human communication.

Works Cited

Witcher, Kimberly. " Option 1 - Research on Topics In Information Security."

1. 4c.

February 17, 2005. www. sans. org. Web. 11 December 2009.