Interception of Wireline Digital Signals Using Electromagnetic Fields

Joel Hill, Devon Haubold, Qammer Gul, Mohamed Bedru

April 17, 2016

Contents

1 Introduction

In a wired network, security is often focused on protecting the endpoints. Routers are kept behind lock and key, and when necessary ethernet ports are hidden or disconnected. The data itself can also be encrypted, a security layer that can be found in local network communication, as well as across the web. There are many cases however, where the encryption of data across a wired connection is not practical or is assumed to be unnecessary. The focus of this investigation was on these types of connections: unencrypted data sent from one computer to another over a wired connection.

Data can be sent over a physical connection using electric or optical signals. It has been shown that the data sent through fiber optic cable can be intercepted by bending the fiber optic cable enough for a small amount of light to escape. This escaped light can be read and parsed, thus allowing for undetected interception of data.

An electric signal is not so easily intercepted without detection. It is possible to splice in and hardwire a connection, however this a time consuming process and may result in the detection of the third party. An ideal solution would be quick to implement, have little to no effect on the existing network, and portable.

It has been hypothesized that wired electric signals can be intercepted by detecting the magnetic fields generated by the change in current as data is transferred.

2 Fiber Optics Interception

As most wired signals transport method shifts from the traditional copper wire to optic fiber, the security threat and vulnerabilities grows as the same time. There was a time optics fiber was considered the most secure and most reliable means of network data transmission. This is not the case anymore as more advanced and cheap way of interception and intrusion are developed. However, fiber optic is still a preferred way of transporting big data due to two reasons. One reason is that it transports big volume data very fast. The second reason is its ability to transport data for a long distance with little loss. Law enforcement Agencies, Intelligence agencies, Defense, Telecom Service Providers and Cyber Security are already using devices which can tap optic fiber cables to select, extract and monitor data. One example is the recent leaks which shows how NSA tap the undersea cable (The Atlantic, 2013). It is worse when information is accessed by criminals or those who want to inflict harm on us. It has been proved that a very cheap clip-on coupler can be used by individuals to easily tap a fiber (Opterna For Enlightened Networks, n.d.).

2.1 Vulnerabilities

ptics fiber data transmission used to be very secure as it was very difficult to intercept the transmission. It was also very easy to detect if there was any interception. The methods and devices used to tap into optical fiber were very expensive. It was not easy and realistic for ordinary person to intercept into optics fiber. That is not the case anymore as the technology to intercept into this data transmission become inexpensive and easily available. Some of the vulnerabilities and methods used to tap are as follows:

2.1.1 Curving

It is possible to make the detectable amount of light to leak the optical fibers by bending the fiber. By using the right device to detect and capture the leaked light, the data transmitted can be accessed. To get full data passing through the wire, only small leak of the light is enough. This method works well on low speed data rate and not good for high speed data rate (SANS Institute Reading Room, 2005)