

Danger: Fiber Optic Intruder



INFORMATION WARFARE SPECIALISTS ARE EXPLORING NEW WAYS OF PROTECTING FIBER OPTIC NETWORKS AGAINST INTRUSIONS.

By MICKEY McCARTER
MIT CORRESPONDENT

Like many global companies, the U.S. military is showing growing interest in using fiber optic networks to provide more information capability to users. Fiber optic networks are more powerful and versatile than traditional copper-wire networks, operating at very high speeds and providing high bandwidth.

Despite widespread assumptions about their relative invulnerability, however, experts say fiber optic networks are susceptible to intrusions and other security threats. In recognition of the increased reliance on fiber optics, the Air Force Information Warfare Battlelab (AF-IWB)

this spring tested an intrusion detection system that could detect taps in fiber optic lines.

AF-IWB is one of seven Air Force battlelabs, all of which support the development of innovative technologies for their particular mission areas.

The recent test ran Interceptor, an intrusion-detection hardware system from Network Integrity Systems, on a fiber optic network at Scott Air Force Base, IL, as part of an Air Force test called the gigabit Ethernet multimode fiber intrusion detection system (GEMMFIDS). The Air Force had published an industry request for

proposals regarding technologies that could monitor the active signal of a multimode fiber strand to detect signal degradation or power disturbances that could indicate physical intrusion.

“Unique among Air Force battlelabs, AF-IWB receives more than 70 percent of its initiatives as concepts from industry,” explained 1st Lieutenant Brian Hermann. “After a rigorous screening process, which weeds out over 85 percent of those submissions, Network Integrity System’s submission received approval as a Battlelab initiative in June 2003. Concepts selected for demonstration by AF-IWB must show operational impact for the Air Force, wide breadth of application and low degree of technical risk.”

CAPTURING THE LIGHT

The risks associated with fiber optic

networks are not widely understood, according to Joe Giovannini, Network Integrity Systems vice president of sales and marketing.

“In fact, cable companies for years have sold as one of the values of fiber cable that it could not be tapped,” Giovannini explained. “They based this on emissions of information. The way fiber operates is that light pulses are sent down the core of the fiber, and those pulses are basically a digital signal, on and off, that transmits and interprets data. But the physics of optical fibers are such that if you bend them to a certain radius, some of that light actually escapes out of the fiber.”

Intruders can capture light pulses that escape the fiber through a number of devices available on the market, Giovannini said. Because most of the intrusion detection systems for fiber optics are not sensitive enough, intruders could read information from a fiber optic network without the knowledge of its administrator or users, he added.

“Information assurance and computer network defense are essential in today’s high-tech world,” Hermann said. “As sub-disciplines of information warfare, innovative concepts in these areas will continue to be considered for possible demonstration with the AF-IWB.”

Network Integrity Systems, a small business based in Conover, NC, has developed the third generation of Interceptor, a portable hub-shaped device, to detect physical taps in optic networks. With GEMMFIDS, AF-IWB hosted demonstrations with the 868th Communications Squadron to examine technologies that could do just that.

Although Interceptor detects signal degradation or power disturbances, it does so by looking at the characteristics of the power, and not the actual strength of the power, Giovannini said.

Light transmission over optics is measured in dBm, which refers to the strength of the decibels of light, a concept similar to decibels of sound. Traditional means of monitoring a fiber optic network focus on attenuation monitoring, which measures the loss of optical power during an event. The attenuation of optic power would indicate a bend or break in a fiber line, alerting operators to the possibility of a tap in that line. However, attenuation monitoring is not good enough for the needs of the military, Giovannini said.



Joe Giovannini, Network Integrity Systems vice president of sales and marketing.

“Typically, the power of the light in an optical fiber is about 300 microwatts,” Giovannini said. “The receivers that are used in optical taps only require about 400 nanowatts of optical power to interpret a single. If you take a 300-microwatt signal and bleed off 400 nanowatts of power, you have only lost what equates to a loss of dBs of less than 0.01 dB.”

Attenuation monitoring products cannot detect a loss that small, Giovannini said. After testing some popular attenuation-monitoring products sold in stores, Network Integrity Systems discovered that the attenuation had to be from two to 10 times greater than 400 nanowatts for the products to detect it.

As a result, skilled intruders could tap a fiber optic network and never alert the attenuation-monitoring products to their presence. The Interceptor system uses a proprietary method to examine the characteristics of the light traveling through the fiber, which it can use to detect the loss of very small amounts of power.

For competitive reasons, Giovannini declined to discuss exactly how Interceptor works, saying only that the device uses a number of techniques. To prevent false alarms, the system filters the signal through signal-processing software that recognizes intrusion-detection signatures and distinguishes them from events that are not a threat.

“When an Interceptor system is installed on a network, it runs through a user-determined length of time configuration cycle, where it undergoes this smart filtering in order to learn what the normal disturbances on the fiber are going to be,” he said. “Because our system is so sensitive, if the fiber vibrates as a result of an elevator that may be going up and down a shaft next to the cable route, for example, that could trigger alarms. Through our proprietary smart-filtering technology, we learn about that elevator

and the impact it has on the fiber, and that then is filtered out and not alarmed.”

DISTURBANCE DETECTED

AF-IWB does not endorse specific products, according to Air Intelligence Agency spokesman Masao Doi. The battlelab does not even conduct full-scale testing of products, instead running demonstrations to provide senior Air Force officials with concepts of what does and doesn’t work.

Even so, Hermann reported the following from the test: “The GEMMFIDS demonstration did what Network Integrity Systems claimed it would do—detect a physical disturbance on a multi-mode fiber optic cable. The AF-IWB handed the concept off to the Air Force Communications Agency for further evaluation.”

AF-IWB is responsible for briefing the results of demonstrations such as GEMMFIDS to senior Air Force leaders as well as the Air Force acquisition community. “These recommendations help determine whether or not the AF will procure the item, move forward with an idea, or wait for further technological improvements,” Hermann said.

Giovannini added that Interceptor was also involved in an Army beta test that showcased its value to the Air Force. A campus that maintained a secure fiber optic network for use by warfighters had a cable that ran outside from one building to another. The established Army approach to securing the fiber optic cable was to make it inaccessible to would-be intruders by encasing it in concrete.

“That user would have had to spend tens of thousands of dollars encasing the cable in a duct filled with concrete,” Giovannini said. “It’s a term called hardened carrier.”

This Army command hoped to skip the expense involved in encasing the cable, and also wanted access to the cable in the future. By encasing it in concrete, not only would the Army prevent intruder access, it would prevent legitimate access for purposes of doing further work with the cable, Giovannini said. ○

Comments and Letters to the Editor about this story are encouraged. Contact Editor Harrison Donnelly at: harrisond@kerriganmedia.com