

Hacking at the Speed of Light

Apr 1, 2006 12:00 PM

By Sandra Kay Miller

http://securitysolutions.com/mag/security_hacking_speed_light/

BREACHING FIBER-OPTIC CABLES was the leading plot in Tom Clancy's novel, "Power Plays: Cutting Edge." Fiber-optics have also occasionally been tapped covertly on prime-time TV dramas about special operations and secret government agencies.

However, it is an issue that is as much fact as fiction. News about fiber-optic vulnerabilities and threats have remained in the shadows despite being around for a number of years.

Organizations such as financial, healthcare, insurance and publicly-traded companies that must adhere to regulatory compliance have not even begun to address the fact that delivering private and sensitive data over fiber-optic communication systems is vulnerable to being captured virtually undetected. It is not just the military eavesdropping on the optical networks of terrorist-harboring countries to pre-empt attacks. Every day billions of dollars worth of business travels across fiber crisscrossing the globe. Hackers have the ability to exploit the optical network to glean information or inject data nefariously, such as with denial of service attacks, which can bring networks to a grinding halt.

Gartner's Distinguished Analyst John Pescatore, former NSA-trained U.S. Secret Service security engineer, openly commented in 2003 about the tapping of fiber optics over the last decade. He also pointed out at that time that avoiding detection and processing the collected data presented a greater challenge than the one presented by common hacks that security teams must routinely contend with today, which frequently target data such as personal information and credit card numbers.

In the mid-1990's, reports surfaced of the NSA covertly splicing into a Flag Telecom's undersea fiber-optic cable. Air Force Lt. General Michael Hayden (now retired), director of the NSA at the time, neither denied nor confirmed the allegations, but he did comment about the challenge of distilling the huge amount of data collected into useful intelligence.

There have been sporadic reports of tapping fiber-optic cables such as the eavesdropping device illegally installed on Verizon's optical network in 2003. According to The Wolf Report in March 2003, the intent of the device was to glean information from a mutual fund company regarding its quarterly statement prior to its public disclosure. In 2000, Deutsche Telekom suffered the breach of three main trunk lines at Frankfurt Airport in Germany.

Easy target?

Originally, fiber-optic cables were considered one of the most secure forms of communication infrastructure, but according to Kimberlie Witcher's research paper published by the SANS Institute in 2005, "In the last few years, it has been suggested that fiber is almost as easy to tap as copper."

Tapping into fiber no longer requires the use of a submarine or a multi-million-dollar project funded by government security agencies. While Witcher points out the task of hacking fiber is not easy, she does believe that armed with the right tools and knowledge, an experienced hacker could perform such an intrusion. Increasing computing power and new sniffing tools have also facilitated easier optical hacks compared to the NSA's early research.

Hacks on optical networks are achieved by extracting light from the ultra-thin fibers. The first step is to acquire access to the targeted fiber-optic cable. There are literally hundreds of million of miles of fiber cable throughout the world, with over 90-million miles in the United States alone. While much of this cabling is difficult to access — undersea, buried underground, encased in concrete, run through walls and elevator shafts — there are plenty of cables readily accessible. Some cities, such as Roanoke, Va., have posted detailed maps of their fiber-optic cable infrastructure on the Internet in an effort to get businesses to hook into the system. Pescatore estimated that enterprises have as much as 75 percent of their network cabling in publicly accessible areas. Once a target has been identified and accessed, the next step would be to extract light, and thus data, from the cable.

The easiest and most undetectable method for optical hacking is bending. Using a commercially available clip-on coupler, a micro-bend is placed in the cable to allow a small amount of light to radiate through the polymer cladding. This light, and thus the data, is then captured with a photodetector. An inexpensive optical/electrical converter can then support a connection to an Ethernet network interface card. Once a successful tap has been accomplished, sniffer software can capture packets and apply filters to the data for IP and MAC addresses and DNS information.

Another optical hacking method — splicing — is much trickier to perform undetected. Corning Fiber Optic Engineer Wayne Siddall explains that when a splice in the fiber is made, the light is momentarily cut off, causing an interruption in service that would be noticed by the operator. When cables are capable of carrying 100-million connections at a time, an interruption of a millisecond results in re-routing transmissions to maintain network integrity, thus alerting technicians to investigate a potential problem.

Detection and prevention

Despite the billions of dollars spent annually on information security, a select set of vendors have begun developing tools for protecting optical networks. These solutions offer intrusion detection and prevention at the physical level. They can identify and alert operators to optical events including malicious intrusions, cable

breaks, receiver overloads, weak optical signals, data signal loss, transients and loss of power.

Opterna (www.opterna.com), a Quakertown, Pa.-based company, offers a rack-mounted fiber intrusion detection system (IDS), the FiberSentinel System, which provides passive real-time, protocol agnostic monitoring for optical networks. Based on artificial intelligence technology, intrusions can be automatically detected and shut down while traffic is simultaneously re-routed to an alternative path.

Established in 2001 and headquartered in New York, Oyster Optics (www.oysteroptics.com) has developed bleeding-edge technologies for optical security and monitoring. Seth Page, chairman of the board at Oyster Optics, says that most CEOs and CIOs today have little or no knowledge about how easily someone could tap into their optical networks. Recognizing the impact from threats such as eavesdropping, corporate and government espionage, network disruption and even terrorism, Oyster Optics' vendor-neutral, protocol-independent solution has been deployed by communication equipment vendors in both commercial and government sectors.

Increasing risk

The growth of companies such as Oyster Optics and Opterna suggests that the risk of having someone tap into optical networks is increasing. An intelligence-gathering method once reserved for military surveillance and international espionage can be accomplished using commercially available tools.

These hacks render useless traditional network security solutions, such as IDS, IPS and firewalls.

At this point, the only thing that will prevent information from being poached would be encrypting transmitted data.

Considering the lengths at which an intruder will go to surreptitiously access an optical network for disreputable purposes, chances are good that they will also include encryption-breaking tools in their arsenal.