

## Optical Illusion

[http://informationsecurity.techtarget.com/magItem/0,291266,sid42\\_gci1228170,00.html](http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1228170,00.html)

by: [Sandra Kay Miller](#)

Issue: [Nov 2006](#)

*Fiber-optic networks aren't hack-proof: A savvy attacker can crack them with ease.*

**You know that** your copper-wired networks and wireless LANs can be sniffed and that your data can be compromised. But fiber-optic networks are a different story, right?

Not really. Despite their reputation for being more secure than standard wiring or airwaves, the truth is that fiber cabling is just as vulnerable to technical hacks using easily obtained commercial hardware and software.

There have been few public reports of fiber hacks: In 2000, three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany. In 2003, an illegal eavesdropping device was discovered hooked into Verizon's optical network; it was believed someone was trying to access the quarterly statement of a mutual fund company prior to its release—information that could have been worth millions. International incidents include optical taps found on police networks in the Netherlands and Germany, and on the networks of pharmaceutical giants in the U.K. and France.

Those high-profile fiber intrusions offered few details. For the most part, these hacks often go unreported as well as undetected.

Tapping into fiber-optic cables originally fell into the realm of national intelligence. Take the 2005 christening of the USS Jimmy Carter, a \$3.2 billion Seawolf-class submarine specifically retrofitted to conduct "signal intelligence"—military-speak for monitoring communications by tapping into undersea cables.

As recently as 2003, John Pescatore, Gartner VP distinguished analyst and a former NSA-trained U.S. Secret Service security engineer, said that while fiber-optic cable hacking had been taking place for nearly a decade, avoiding detection and processing the stolen data was much more difficult. Things have changed. In a research paper published by the SANS Institute in 2005, Kimberlie Witcher notes that industry experts now believe that fiber is almost as easy to tap as copper. And, tapping into fiber no longer requires a submarine or a multimillion-dollar project funded by government agencies. The required equipment has become relatively inexpensive and commonplace, and an experienced hacker can easily pull off a successful attack.

"You can jump on the Internet right now and buy a tap for about \$900," says Andy Solterbeck, VP and general manager of the data protection business unit at SafeNet, an encryption company that has been experimenting with hacking fiber-optic cables. "We've done this in our labs. We've demonstrated this at Interop. We've shown people that this kind of threat exists."

## Light Exploits

Setting up a fiber tap is no more difficult than setting up equipment for any other type of hack, wired or wireless: It's based on hardware, software and knowledge.

Optical network exploits are accomplished by extracting light from the ultra-thin glass fibers. The first, and often easiest, step is to gain access to the targeted fiber-optic cable. Hundreds of millions of miles of fiber cable stretch across the globe; there are more than 90 million miles in the United States alone. Although most of this cabling is difficult to access—it's underground, undersea, encased in concrete, and run through walls and elevator shafts—plenty of cables are readily accessible for those willing to look. Some cities, for example, have detailed maps of their fiber-optic infrastructure posted online in an effort to lure local organizations to hook into the network.

After homing in on the target and gaining access to the cable itself, the next step is to extract light and, ultimately, data from the cable.

Bending is the easiest method. (See *"Fiber Hack," at right.*) It is also the most undetectable, since there is no interruption to the light signal. Commercially available clip-on couplers cost less than a thousand dollars; these devices place a micro-bend in the cable, leaking a small amount of light through the polymer cladding.

Once the light signal has been accessed, the data is captured using a photo detector—a transducer capable of translating an optical signal into an electrical signal. They're listed on eBay for around \$500.

Also on eBay for the same price is the next piece of equipment needed to sniff data off of glass—an optical/electrical converter. This device facilitates the connection to an Ethernet network interface card. Once a successful tap is in place, freely available sniffer software can begin capturing packets and filtering data for information such as IP and MAC addresses, DNS information and keywords in data passed in the clear.

Splicing, another method, isn't practical; it often results in detection due to the momentary interruption of the light signal. According to Wayne Siddall, an optical engineer with Corning Fiber, the operator would notice this type of interruption in service, even for a millisecond, because cables capable of carrying 100 million concurrent connections require instantaneous signal rerouting to maintain network integrity. And, commercially available splicers are expensive—about \$7,000 to \$9,000.

## Light Shields

A few vendors are developing tools that protect optical networks, offering intrusion detection and prevention at the physical layer. They 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](http://www.opterna.com)) sells the FiberSen-tinel System, a rack-mounted fiber IDS that offers passive real-time, protocol-agnostic monitoring for optical networks. Intrusions are automatically detected and shut down while traffic is simultaneously rerouted to an alternative path using artificial intelligence technology.

Another fiber IDS solution, Fiber SenSys from CompuDyne ([www.compu.dyne.com](http://www.compu.dyne.com)), has become popular in government and military installations, airports, oil refineries, electrical substations, nuclear power plants, water purification and storage facilities, corporate headquarters and manufacturing centers—even palaces—throughout the world.

Oyster Optics ([www.oysteroptics.com](http://www.oysteroptics.com)) has been developing bleeding-edge technologies for optical security and monitoring since 2001. Oyster Optics' vendor-neutral, protocol-independent solution re-duces the risk of threats such as eavesdropping, corporate and government espionage, network disruption and terrorism.

At this point, these detection solutions notwithstanding, the only measure to prevent information from being pilfered off of optical networks is the encryption of transmitted data.

"I think we've seen large increases in the use of encryption over all network paths, including fiber-optics—and encryption defeats eavesdropping," says Gartner's Pescatore.

"In general, I think security has moved up a notch, and tapping into fiber for eavesdropping is still a more difficult way to get at information than many other paths," he says. "But, our advice to enterprises is to use encryption over all network connections where the physical security of access to the network, whether copper or fiber or wireless, cannot be secured."

Many organizations make the mistake of encrypting the data and the transmission, which is redundant. If the data is encrypted, there is no need to spend extra money to send it through a secured tunnel. The trend is leaning toward encryption at the data layer, which reduces the latency and overhead associated with transport.

### **An Open Front**

The criminal threat continues to grow: Consumer Affairs estimates that in 2005 more than 50 million Americans received notification that their personal data was stolen due to a data security breach. The FBI Cybercrime unit estimates that more than \$100 billion a year is lost through corporate espionage.

To counter this, billions are spent on information security products. The SANS Institute listed the federal government's 2006 IT security budget alone at \$1.685 billion—up 7.2 percent from 2005.

Unfortunately, optical hacks render most traditional security methodologies ineffective. Financial, health care, insurance and publicly traded companies saddled with regulatory compliance rarely consider that private and sensitive data delivered over fiber-optic communication systems is vulnerable to being captured through virtually undetectable hacks.

Your data transmissions may have already been compromised without your being aware of it. Secur-ing fiber-optic transmission can be costly and difficult, and the bad guys, as usual, have a head start.