Hacking Fiber optics easier than copper cable

Sachin Jung Karki
Freelance IT Security professional
February 1, 2016

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.

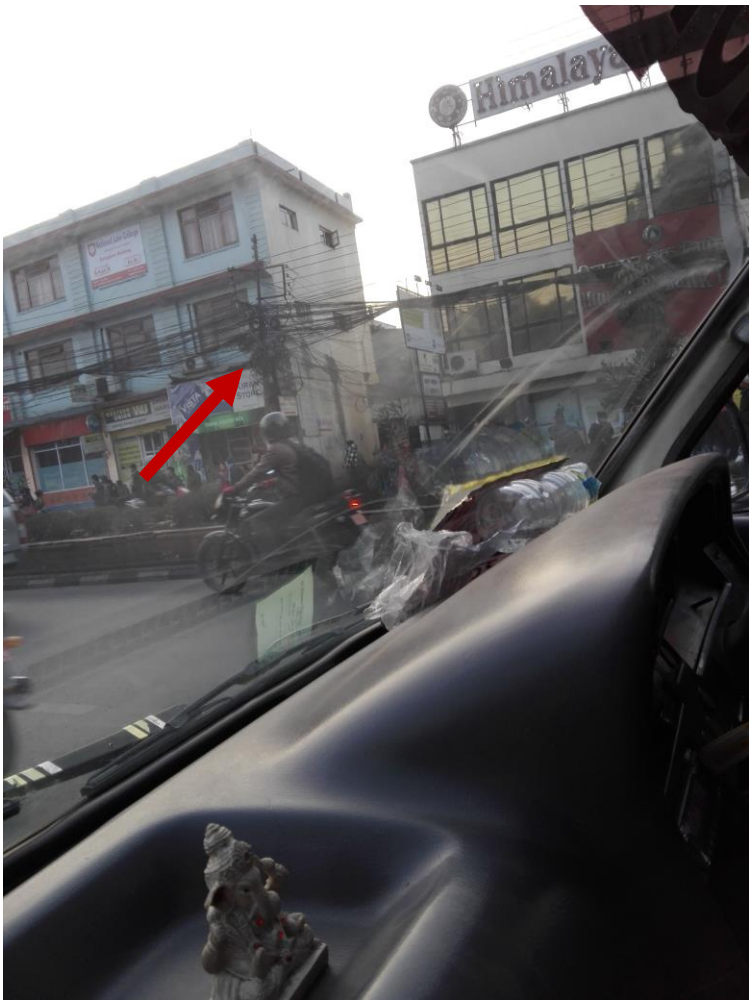
There have been few public reports of fiber hacks: In 2000, three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany. In 2003, an illegal eavesdropping device was discovered hooked into Verizon's optical network; it was believed someone was trying to access the quarterly 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.

We look into this seriously

We have done some workout to get the feedback of the people and service providers. I along with 3 other guys take a van, put some fiber support kits, a steel ladder, some helmets, safety clamps, and gloves and went to a tour around Kathmandu. We have visited several fiber junctions, opened couple of them but didn’t do any harm or eavesdropping and waited to see people’s response. I am amazed that nobody has asked us for whom do we work for, whose fiber is this or are you from any ISP. Below are some glimpse of what we have done and found that almost every fiber is vulnerable in Kathmandu. I found that our commercial, government, health and finance sectors are claiming to be secure or planning to be secure but still they don’t know that their own fiber cable can be tapped so easily.

The above pictures are from Jawalakhel, in front of a complex and opposite to Staff College. The bellow image is from Himalayan Bank, Pulchwok and I bet you can hardly tell which fiber belongs to whom. The same situation can be found from the Ratna Park to Baneshwor, Durbarmarg, etc.

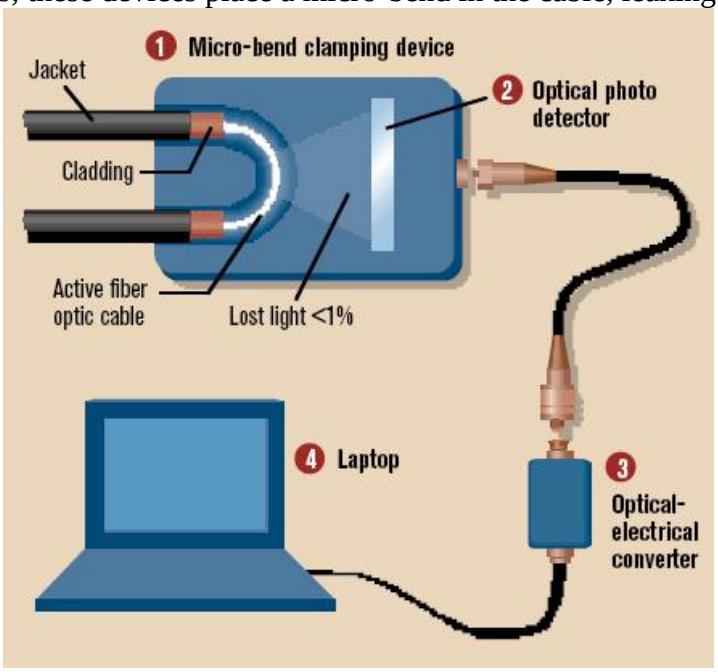


The below image is from Nepal Investment Bank Limited, Durbarmarg and as you can see at the background there is an internet service provider or telecom’s base station and you cannot tell whom these fiber belongs to.

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.

The easy way

Unlike the curve method, this method requires no interfering with the fiber cable. Instead, sensitive photo-detectors are placed around the optical cables. These detectors are used to capture the small amount of light that naturally radiates off the cables (called Rayleigh scattering). Hackers can get the information without physically touching the fiber or even the light signal itself. The light is then amplified by the photo-detector until a sufficient intensity is reached, or can also be redirected through another optical fiber.

Once a successful tap has been accomplished, a packet sniffer software like Wireshark or Burp Suite, etc. that records, monitors, and analyzes the data can be used to capture all data transmitted. Readily available spectrum analyses even make users of optical multiplexing techniques, such as wavelength division multiplexing (WDM), vulnerable to attacks.

How to protect your Optical Network

As it is impossible to monitor the entire optical fiber network, the only real preventive solution to protect information is to encrypt the data before it goes through the network. At this point, the only thing that will prevent information from being poached for industrial espionage is if the encryption renders the data acquired unusable by the hackers. Due to the sensitive nature of the information carried being from financial institutions, insurance companies, public administration, or in the pharmaceutical and chemical industries it is paramount that the privacy and reliability of the information carried are guaranteed, as the stakes and risks involved are high. Some large organizations have already been subjected to data theft through their optical fiber networks in the last few years. Here are a few examples of breaches to illustrate the risks of optical tapping:

1. Security forces in the United States discovered an illegally installed fiber eavesdropping device in Verizon's optical network. According to the white paper Wolf Report, "Das Schweigekartell I & II," March 2003, the device was placed at a mutual fund company shortly before the release of their quarterly numbers.
2. The white paper also reports that the former East Germany's secret service (STASI) had been tapping the optical networks between the former West Germany and West Berlin. About 4.2 million credit and debit card details from supermarket chain Hannaford were reported stolen according to a story published by the Wall Street Journal in March 2008. With 1,800 reported cases of fraud, the breach remained undiscovered for three months and took 10 days more to contain.

3. The U.S. government has set up secret rooms at AT&T (WorldNet) and has capability to eavesdrop on networks worldwide, according to the May 17, 2006, issue of the W*ired* magazine.
4. According to a story published in the November 15, 2006, issue of the *Information Security Magazine*, criminals are illegally monitoring Dutch and German police networks, and the networks of pharmaceutical giants in the United Kingdom and France.
5. The same article reports that three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany.

ESSENTIAL GUIDANCE

Despite millions of dollars spent every year on network security, only a handful of security vendors address the risk of data theft through the optic fiber cable network. Several Companies, such as Swiss vendor InfoGuard AG, offer such solutions with their Layer-2 encryption appliances. InfoGuard's range of appliances is capable of handling encrypted data traffic between sites of various sizes. The products can handle data traffic up to 10Gbps across most environments. The data is encrypted using the Advanced Encryption Standards (AES) supporting key sizes of 128 bits or 256 bits with wire speed (maximum data transmission rate) throughput and latency time in the microsecond range.

Human error

There is a strong need of awareness programs to be provided for general public, government, health and finance sectors, etc. All public personnel must be aware about these hacks and law enforcement agencies and organizations must organize these kinds of awareness. Open fiber junctions, easily accessible fiber distribution pods, unsecure fiber communications will lead to not only information and data loss but also might cause your organization’s reputation and trust lose. Imagine a bank’s fiber has been hacked and information is published into internet or imagine government’s data has been tempered by sniffing and taping of fiber. These are some scenarios on which general public will panic and they all come to you to get their money back which might cause banks to close their business, government utility will be no more secure, people might be angry and stop taking ISP of any service providers service. Ultimately this will cause our economy fall and our policies, system may fail. As a genuine citizen of this country I would like to contribute to provide awareness but government are you ready.