Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND

German original published in: Frankfurter Allgemeine Zeitung, March 13, 2002, Number 61 / Page 14

EXTRA! EXTRA! HOW EASILY OPTICAL FIBERS CAN BE TAPPED

by Heinz Stüwe

BONN, GERMANY - Telecommunication companies would prefer to hush-up the problem up. Information is also very sparse from other enterprises. That's no surprise. The blatant question that needs to be answered: Is the backbone of modern communications vulnerable? A categorical "No" would hardly be a convincing answer for the technical laymen. The successes of computer hackers have made headlines often enough. PC users are terrified of new virus warnings after experiences with computer viruses such as "I love you". Radio conversations and cell phone calls can already be intercepted. One must then also consider the actual information superhighways, that is, the fiber optic routes. Around 300 million kilometers of this light-wave-medium encircle the globe, according to estimates. They allow high transfer-rates and are therefore a particularly efficient communication medium for data, images and voice. Moreover, optical fibers are seen as especially secure in contrast to conventional copper coaxial cables. This is incorrect, says Seth R. Page, the leader of Oyster Optics, Inc. in New York City, a young company that offers security solutions for such optical networks. He is of the belief that fiber optic cables are actually extremely vulnerable.

As an example, the American quotes an event from recent German history. When the German Federal Post laid fiber optic cables between West Germany and Berlin, the East German State Security (STASI) had already tapped the lines before they were even in service, as it later became clear after the German Reunification. The eavesdroppers of the East German State Security's main-department were also engaged in economic espionage - a very real topic then, as it still remains today. The damage caused by economic espionage for American business alone is estimated at one hundred billion dollars annually. One fifth of which can be attributed directly to the espionage of company secrets through technical methods of various types. In addition, numerous state intelligence agencies gather information on behalf of their local industry.

The undetected and illegal eavesdropping of fiber optic cables around the world is everyday practice, according to Page. It is easy, inexpensive and the risk of being discovered is low. Experts confirm that the tapping of fiber optic cables does not represent a big problem technically. One doesn't even have to cut the optical fiber transmitting the light waves, which would normally disconnected the optic signals at least for a short moment. When an optical fiber is bent, leaking light can be intercepted with a photocell. This principle is used by so-called bending-couplers, which direct the leaking light, for example, into a different optical fiber. Such optical test equipment, used by telephone-companies, can be bought for 500 to 1200 dollars freely and fully legally.

Deutsche Telekom, however, in regards to their own fiber optic networks, considers "the highest security as a given," as expressed by a company spokesman. Up until now there have been no reported cases of optical taps, he says. Deutsche Telekom, as their own key witness, has proven otherwise, Page counters. He points to the European Patent (EP 0 915 356 A1) issued on the 12th of May 1999. Under

this publication number, the "method and device for the extraction of signals out of an optical fiber" was patented. Owner: Deutsche Telekom AG. Inventor: Herbert Walter, Ph.D. An identical patent was granted to the Deutsche Telekom on the 24th of July 2001 in the United States. "The extraction of signals with bending-couplers is technically simple and therefore easily to use, but, because of the unavoidable reduction of the signal, the tapping can in principle be noticed", it is written in the official description. With this invention it is possible to extract signals without measurably influencing the signals transmitted through the fiber optic cable. "This is accomplished by the already existing lateral scattering processes (Raleigh-Scattering), whereby leaking light from the optical fiber is directed to a photo-detector." In plain English: Deutsche Telekom has patented an eavesdropping device that doesn't even need to touch the optical fiber.

According to information from the German Federal Office for the Security of Information Technology (BSI) in Bonn, fiber optic cables are in fact not secure against eavesdropping. That is why the encoding of data is so important. Cryptology doesn't solve the problem however, argue critics. Encryption is a problem that can be solved mathematically. Furthermore, hardware and software for decryption is freely available.

The New York company founder, Page, wants to convince telephone companies and equipment manufacturers of a technical solution, that enables the tapping of optical fibers to be immediately determined, along with the precise location of the tap. It is based on phase modulation, a change in the optical signals. The enthusiasm of the industry is limited. Neither the suppliers nor the operators of fiber optic networks want to admit that their technology is not secure. With the weak business outlook around the world and a bad climate with the stock exchanges, bad news now is extremely inconvenient for the telecommunication industry. Regulations for especially secure facilities exist only within the ‘secret economy’, the defense industry - but not for banks and their data cables to outsourced data processing centers. One can only point to the risks, says the BSI. The companies themselves have to consider the consequences.