

## **NETWORK WORLD NEWSLETTER: M. E. KABAY ON SECURITY**

**March 4<sup>th</sup>, 2003**

**Today's focus: Tapping fiber optics gets easier**

By M. E. Kabay

Security experts have known for decades that fiber-optic cabling can be tapped for interception of communications. But until recently, such taps have been viewed as largely impractical.

The equipment was expensive and the number of fibers in the cables made it difficult to narrow down captured transmissions to a particular connection. In addition, physical interruption of the fibers could be detected using time-domain reflectometry, making such taps hard to conceal. It was also known that teasing apart the fibers and bending them in a tight curvature would allow escape of a small portion of the signal without revealing the data interception. Nonetheless, fiber-optic cabling was viewed as largely secure against wiretaps.

I recently received an interesting paper on recent developments in optical fiber taps from Seth Page, CEO of Oyster Optics, a provider of optical security, monitoring and intrusion-detection products. He has very kindly permitted me to quote from his paper.

Page writes that the situation has changed:

"For both public and private networks, optical taps and analytic devices are required and inexpensive maintenance equipment in common use worldwide today. Various types of optical taps, however, both off-the-shelf and customized, are also used for corporate espionage, government espionage, network disruption and other potential terrorist-type activities. Used nefariously, optical taps allow access to all voice and data communications transiting a fiber link. Modern commercial network equipment and network configurations cannot detect most types of optical taps."

"Optical taps that are used illicitly to garner information are most often placed in the access or local loop for a number of reasons. Firstly, 100% of all information entering and exiting a building, campus or local area can be obtained by tapping between the customer premise and the first network switching node or central office, from where it might then otherwise get switched along divergent routes. Secondly, network configurations, bandwidth and speeds are more manageable towards the edge of the network, implying less expensive equipment and a simpler penetration. Thirdly, opportunities for direct access to fiber are easier to locate, simpler to identify and more plentiful in the public and private spaces that provide such fiber-routes. Such spaces include: telco closets; cages; risers; basements; conduits; car garages; drop-down tile-ceilings; and pathways in subways, tunnels and across bridges, to name few.

"A successful tap can be achieved with merely an optical tap, packet-sniffer software, an optical/electrical-converter and a laptop. Packet-sniffer software filters through the packet

headers, only extracting those packets which match a specific telephone number, IP address or other characteristic. Gathered information is then stored locally or forwarded to the intruder through various mechanisms, including wireless, another optical or copper line, another wavelength or channel, or other means."

Clearly, physical protection of optical transmission media and junction boxes is essential; in addition, data encryption plays a role in protecting sensitive data.

Page points out that encryption can add cost, performance and compatibility problems to data communications and cannot help to identify the existence of a tap. His company has apparently developed methods for helping to protect optical data transmissions against such taps and to spot the existence and location of the taps quickly. I haven't seen the details yet, but anyone interested in these issues is welcome to write to Seth Page directly at <mailto:seth@oysteroptics.com>

The company's resource page can be found at: [http://www.oysteroptics.com/index\\_resources.html](http://www.oysteroptics.com/index_resources.html)

\* \* \*

M. E. Kabay, Ph.D., CISSP, is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, Vt. Mich can be reached by e-mail <<mailto:mkabay@norwich.edu>> and his Web site <<http://www2.norwich.edu/mkabay/index.htm>>.