

## TECHNOLOGY ASSESSMENT

---

### Fiber-Optic Networks: Is Safety Just an Optical Illusion?

---

Romain Fouchereau

---

#### IDC OPINION

---

Fiber-optic cable networks have been deemed the fastest, most reliable, and most secure way of transporting data through the network for decades. This reputation has now been proven wrong for several years with the arrival of new and inexpensive technologies making data theft easily available to hackers.

- In sectors such as banking, insurance, pharmaceutical or government, the data transmitted is of the utmost sensitivity and could have disastrous repercussions if it fell into the wrong hands.
  - Corporate espionage is real and needs to be seriously taken into account in the security plans for every organization. Securing the inside network is not sufficient enough, data going from one site to the other can be intercepted and this security gap needs to be addressed.
  - Strong preemptive encryption solutions need to be deployed on the fiber-optic networks to limit the risk of being exposed to data theft.
-

## IN THIS STUDY

In this study, IDC discusses the fiber-optic cable network technology with a focus on the security threats that can be encountered by organizations that have deployed such networks.

## SITUATION OVERVIEW

Fiber-optic cables are the best way to transport important volumes of data in a fast and reliable way. They are widely deployed in all large enterprises including financial, telecommunication and public sector. It is also very gainful for long-distance communications, because the light propagates through the fiber with little loss compared to electrical cables. They have also the advantage to save space in a building's network infrastructure as fiber-optic cables carry more information data and they also remain unaffected by electrical interferences.

---

### Fiber-Optic Cable Networks Overview

In today's business, transporting data in a fast and reliable way is of the utmost importance and the volume of information traveling on the networks is getting bigger and bigger. With hundreds of millions kilometers of fiber-optic cables running all over the globe, the amount of data going through every second is huge, and it is necessary that the information goes from one place to another in a secure way.

---

### Vulnerabilities in the Network

Optical fiber cables have the reputation of being more difficult to hack than traditional copper cables. This reputation, however, is not justified, although, tapping into optical fiber networks to intercept data or communications is still seen as a very difficult and impractical activity, with the equipment required doing so considered extremely expensive, and the resulting loss of signal makes it easy to detect interceptions. With tapping and hacking technologies becoming easily available to anyone, tapping into fiber cables with very little chance of being detected is becoming easier than before.

Organizations in the financial, insurance, healthcare, and government sectors deliver sensitive information across fiber-optic cables around the world. Hence, capturing or eavesdropping on this data serves not only military purposes. Industrial espionage in these sectors is worth billions of dollars. It must be kept in mind, therefore, that some hackers have the capability to attack and exploit optical networks to collect information or introduce dangerous data that can halt or disable networks.

Most of the networks' cabling is relatively easy to access due to maintenance requirements and often only protected by very weak mechanical means. Once the targeted fiber-optic cable is acquired, hacks on optical networks are achieved by extracting light from the ultra-thin fibers. There are three main types of optical tapping methods:

#### ☒ **Splice method**

Splicing is the most common method to tap into the optical fiber — a break is made into the cable by the device, which can then be used to monitor data. The main problem resulting from using this method is that when the splice is made into the

fiber, the light transmitted is cut off for a very short time and can theoretically be detected by technicians. Because of its very short duration, however, it is most likely to be attributed to a network glitch, greatly reducing the possibility of detection. It needs to be noted, however, that most carriers have preinstalled Y-bridges or splice-points on their fiber networks for maintenance purposes. Hackers can easily abuse these maintenance points.

#### ☒ **Splitter/Coupler method or curve method**

By bending the cable, a small amount of light will escape from the fiber. A hacker with the appropriate photo-detector equipment can then capture this light and the data it carries. Only a very small amount of the light going through the fiber is necessary to get the full data transmitted. Equipment and tools necessary for using this method is readily available and commonly used by maintenance technicians.

#### ☒ **Non-touching optical tapping method**

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 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:

- ☒ 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.
- ☒ 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.
- ☒ 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 *Wired* magazine.
- ☒ 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.
- ☒ The same article reports that three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany.

## FUTURE OUTLOOK

With the ever-increasing volume of data transmitted worldwide, with a certain portion of sensitive nature, it is imperative that enterprises exert efforts to secure their information. Organizations spend a lot of money on more traditional network security, such as firewalls, anti-virus, intrusion prevention systems, messaging security, and data leakage prevention, but with the risks of very sensitive data being stolen or bad data and malware being introduced into the network for malicious activities, the need for protecting the optical cable network is vital. With very little attention paid to these security threats, there is an urgent need for government bodies to regulate on the security issues posed by fiber-optic networks.

## 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.

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.

## LEARN MORE

---

### Related Research

- ☒ *Western European Security Appliances Market Directions 1Q09* (IDC #IS57R9, June 2009)
- ☒ *Western Europe Security Appliance 2009–2013 Forecast and 2008 Competitive Vendor Shares* (IDC #IS04R9, May 2009)

## **Synopsis**

This IDC study discusses the fiber-optic cable network technology with a focus on the security threats that can be encountered by organizations that have deployed such networks.

"Fiber-optic cable networks have been deemed the fastest, most reliable, and most secure way of transporting data through the network for decades," said Romain Fouchereau, research analyst, European Systems and Infrastructure Solutions - Security. "This reputation has now been proven wrong for several years with the arrival of new and inexpensive technologies that enable hackers to easily steal data."

---

## **Copyright Notice**

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit [www.idc.com/offices](http://www.idc.com/offices). Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or [sales@idc.com](mailto:sales@idc.com) for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2009 IDC. Reproduction is forbidden unless authorized. All rights reserved.



IDC is a subsidiary of IDG, one of the world's top information technology media, research and exposition companies.

**Visit us on the Web at [www.idc.com](http://www.idc.com)**

To view a list of IDC offices worldwide, visit [www.idc.com/offices](http://www.idc.com/offices)

IDC is a registered trademark of International Data Group