Deloitte.

Tapping of fibre networks

Deloitte.

Fibre tapping

Summary

This article provides an assessment, based on publicly available articles and material, of whether the architecture and technology of fibre networks are protected against tapping.

Deloitte finds that there is a prevailing, misguided belief that fibre networks are more secure than other media, such as copper and wireless technologies. Fibre networks are vulnerable to tapping through the use of well-known techniques such as man-in-the-middle, re-routing and exploiting protocol vulnerabilities and software vulnerabilities in network devices.

There is also a perception that fibre networks are much better protected against physical interference and the installation of tapping equipment. This is a misunderstanding: fibre networks are at least as vulnerable to physical tapping as traditional copper.

Attackers can use various methods, but at present the least expensive option is using optical splitters or clip-on couplers to bend the fibre, transferring the signal in multiple directions and making it possible to tap into network traffic reserved for others.

Tapping of fibre networks

Fibre networks now comprise a large part of the internet infrastructure. Fibre networks offer great advantages in terms of providing a stable, rapid and scalable network. Many internet providers are either directly or indirectly connected to a fibre network. This is the case because backbone providers have invested in fibre technology to better meet the increasing demand for high speeds and digital traffic.

In addition to internet service providers (ISPs), fibre networks are also accessible by businesses and individuals. Fibre optic cables have been laid underground in Denmark and many other countries to provide this fibre network solution.

The rollout of fibre cables began in Denmark and other countries as far back as the late 1990s. The challenges regarding information security at that time differ from those of today. Enormous volumes of data are now transmitted digitally, containing everything from sensitive personal data to financial transactions and trade secrets.

Tapping is an old practice and has been performed in a variety of ways. This document describes some of the general methods for tapping data traffic, as well as specific tapping methods relating to fibre networks. No longer just reserved for intelligence services or authorities, tapping is now a tool used by criminals and people with malicious intent to achieve their end goals. Different approaches and vulnerabilities apply for all types of transmission media; some of these are sufficiently generic that they can be used independently of the chosen technology. Deloitte is including the general methods for tapping networks in this article, as fibre networks are also vulnerable to these types of attacks.

Generic tapping methods

Attackers can use a range of different methods to obtain unauthorised access to data transmissions, regardless of the applicable technology. A network comprises at least two devices connected by cables or wireless technology.

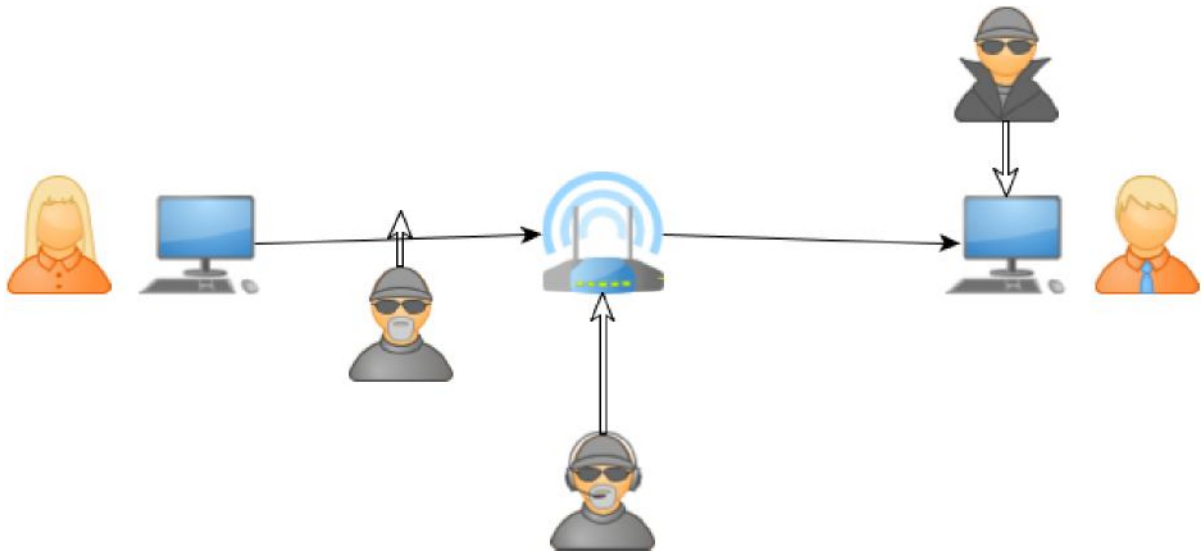
Today's internet-connected devices are composed of many different technologies, ranging from copper cables and coaxial cables to fibre optic cables and wireless technologies such as satellite/radio signals, microwaves, etc. To facilitate all of this, ISPs have invested in a range of hardware for handling data traffic and ensuring this traffic reaches its exit points without a loss of integrity. Standard network protocols have also been established for handling the routing of data traffic from source to destination.

Data traffic tapping can be divided into the following main categories:

- Digital tapping
- Physical tapping

Attackers and authorities employ a variety of tapping strategies, both physical and digital. In this article, Deloitte provides a review of common strategies and methods, and illustrates how confidentiality can be compromised using these techniques.

The following figure illustrates a simplified network that can be tapped by attackers or authorities:



The above illustration is highly simplified but serves to show that attackers can focus on different points of attack to access and compromise data traffic. They can compromise devices that process data or attack weaknesses in network protocols to access data traffic. Attackers can also physically connect to the network cables used to transmit data traffic.

Digital tapping

Digital tapping is achieved by compromising the devices responsible for transmitting, forwarding or receiving data traffic.

Sniffing/Signal interception
Digital sniffing or signal interception is a form of tapping in which attackers use software to access raw data traffic. Commonly available software packages are capable of intercepting all traffic sent

on a cable to which the attacker's device is connected and to store this data in a format that can be inspected and analysed. For example, Wireshark is a well-known product that permits the use of Raw Sockets and features an extensive list of dissection modules to gain structured access to network traffic.

Today's network configurations often manage traffic with the use of switches, which ensure that a device connected to one port in the switch cannot access traffic to another device connected to another port. This can be circumvented, however, with the use of small and inexpensive computer devices such as a Raspberry Pi, which are placed in front of the switch to intercept traffic before it is properly routed by the switch. Many of these devices are the size of a chocolate bar and have impressively strong processing power. It should also be noted that these devices come with an operating system and a large array of input/output options.

In some cases, attackers can also use Address Resolution Protocol (ARP) spoofing, in which a piece of software sends an extraordinarily large number of MAC addresses to the switch. This overloads the ARP table of older or cheap switches and disables dedicated routing to specific ports. Switches impacted by this vulnerability switch over to HUB mode, which means that all devices connected to the switch can see each other's traffic.

Attackers with access to the local network can also use man-in-the-middle attacks such as MAC poisoning, where the attacker takes over the role as gateway for a device, while also taking over the role of device in relation to the gateway.

Re-routing
This attack can be used by individuals with knowledge of IP routing. This type of attack requires that attackers can break into routers and change the configuration so that data traffic is sent through other routers than those originally installed by the ISP. This enables attackers to access data sent over the network, and they can subsequently inspect the intercepted traffic. Back in 2007, it was possible to manipulate the routing tables in routers configured for private use through JavaScript or ActiveX Scripting on malicious websites.

Hardware exploitation
Technically skilled attackers find vulnerabilities in the firmware created by network equipment manufacturers and installed in their devices. These vulnerabilities give attackers the ability to control network devices such as switches and routers, and thus the ability to reroute traffic sent between these devices.

Physical network devices run system software, which often has vulnerabilities similar to operating systems. As a result, manufacturers who take security seriously regularly release patches and updates for this type of software.

These improvements come in the form of firmware upgrades rolled out to devices. However, many devices still in use are no longer supported by manufacturers, while others are never updated at all.

The configuration and maintenance of network devices are also relevant factors. Modern network equipment can be configured for a wide range of uses. Such configuration and maintenance is usually performed by certified technicians. Nonetheless, human error is a common cause of breaches of confidentiality and data integrity. Firewall, router and switch configurations require continuous maintenance; the bigger these configurations, the more administrative work for those who perform configuration changes. A simple error in a firewall or network device can enable attackers to send data to locations other than the intended destination.

Physical tapping

The physical compromising of fibre networks is not as difficult as widely believed. In fact, it is relatively easy and cheap to install a physical tapping device after obtaining access to a fibre cable. The US military commissioned a report back in 1980 about how fibre can be tapped with physical devices.[1]

[1] http://www.thefoa.org/tech/ref/appln/tap-fiber.html

It had long been very expensive to purchase equipment for physically tapping fibre networks, but this has changed dramatically in recent years as a result of technological advances.

Physically tapping a fibre network is essentially a matter of intercepting enough of the light source to enable translation to binary data, while allowing enough light to pass through so that the tapped cable does not show any loss of data.

Tapping can be effectively installed at two locations:

- At the entry/exit points that facilitate the connection to the fibre, e.g. cabinets, hubs or outputs on the recipient's premises.
- On the fibre optic cable itself.

Researchers have explored the possibility of tapping a fibre network. As far back as 1980, confidential studies were performed to explore the possibility of making physical changes to a fibre line so as to access the flow of transmitted data.[2]

Entry/Exit Points

All connections require a starting point where the traffic is initiated and an exit point where the connection ends. The network structure of today is highly complex, with a multitude of different entry and exit points. For example, network providers have invested in highly efficient hardware that can collect large volumes of fibre connections and transmit traffic to other types of networks or to other fibre connections. This makes ISPs a common target for attackers seeking to intercept data. The vast majority of ISPs have invested or rented capacity in an infrastructure featuring a range of measures to secure physical access to routers or switches.

Meanwhile, the exit points must be protected by the buyer of network services. Preventing physical access to the fibre network's exit point is a task for the buyer of network services; depending on cost and type of output, these exit points may be easily accessible by attackers. The problem is further compounded by the relative low cost of hardware that supports the tapping of fibre optic, copper and coaxial cables.[3] These devices are designed to provide insight into the traffic on the network and to prevent abuse of the network's users. An attacker can quickly take such a device and connect it to a Raspberry Pi configured to transmit intercepted data to the attacker. This data can be transmitted through the tapped connection, or more covertly through the mobile network. The price of such equipment is under DKK 15,000. Depending on the target chosen by an attacker, this is a relatively small investment compared to the value that can be extracted.

The following example illustrates how an attacker could establish taps of entry/exit points, based on knowledge of actual attacks on other types of networks/devices:

"An attacker pretends to be a technician from the provider, and claims to need to install/update hardware. The attacker then accesses the entry/exit point (cabinets) and installs malicious hardware. "

This hardware can be hidden in an electrical box and would not be discovered until a technician with knowledge of the setup inspects the installation.

[2] http://fac.ksu.edu.sa/sites/default/files/06149809-Optical Fiber Tapping Methods and Precautions.pdf http://www.thefoa.org/tech/ref/appln/tap-fiber.html https://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-gross-up.pdf https://www.joshruppe.com/fiber-optic-tapping-tapping-setup/ https://www.anixter.com/content/dam/Suppliers/viavi/White%20Paper/Understanding%20Fibre%20Optic%20Network%20Tapping.pdf https://www.dropbox.com/s/fexmecnnb6gq6y6/KevinMitnick EmailHack.mp4?dl=0

[3] https://www.ixiacom.com/products/network-taps-regenerators-and-aggregators http://www.viavisolutions.com/en-us/products/observer-taps-optical

The fibre optic cable

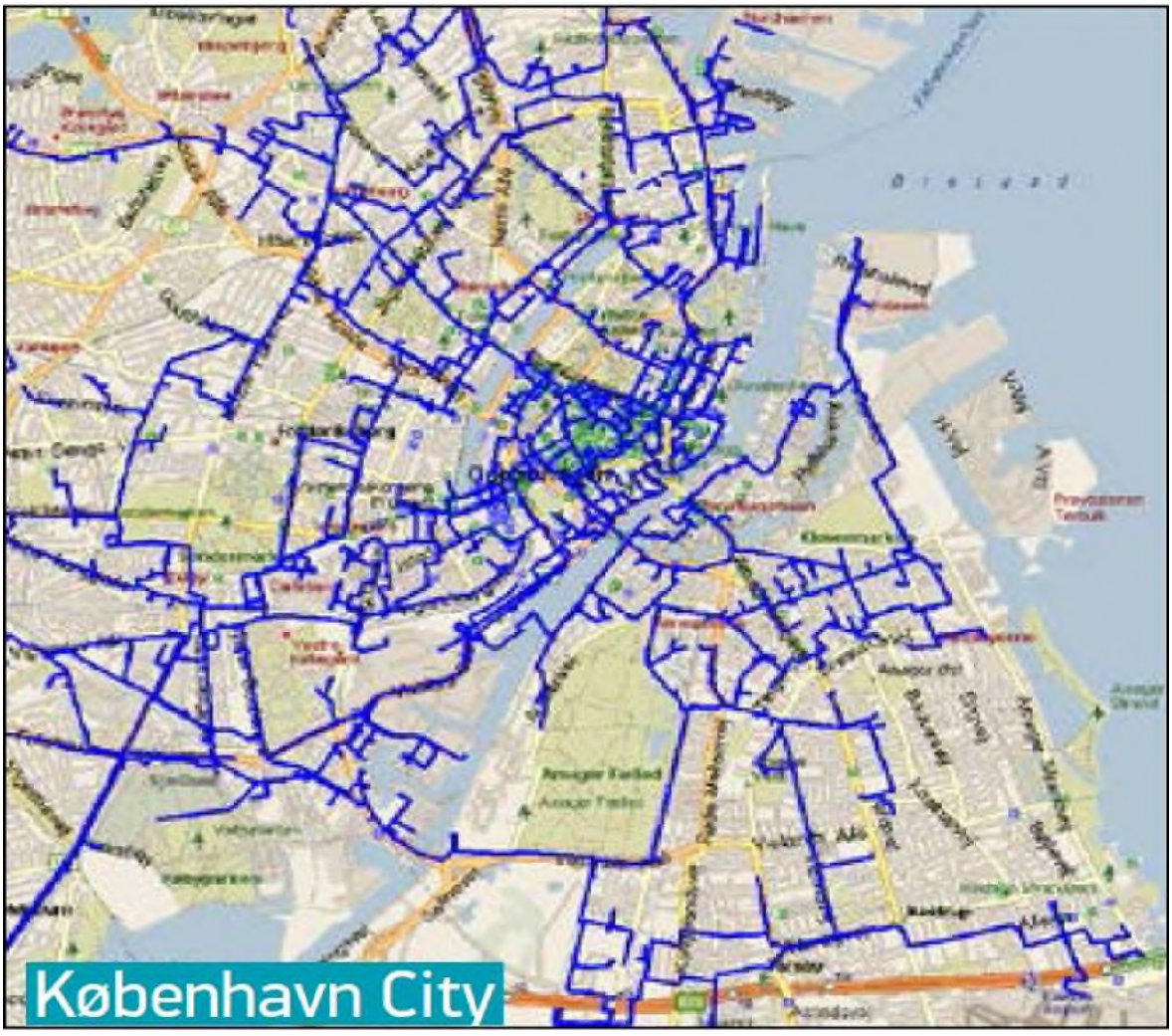
The cable itself is also vulnerable to attack. An attacker who gains access to the fibre cables can utilise some simple techniques to intercept all traffic transmitted through the cable. Fibre optic networks are commonly – and incorrectly – believed to be far more secure than traditional copper or wireless technology.

A variety of methods can be used for tapping, including:

- Bending the fibre.
- Optical splitting.

Other methods can also be used to tap a fibre network, such as capturing lost light, which is difficult in practice, and V-groove carving, which can provide access to some of the light sent through the fibre. However, these methods are not very practical and therefore will not be further explored in this article.

Accessing fibre cables may appear difficult at first, but Denmark alone has countless kilometres of underground fibre cables that can be accessed if an attacker is aware of their location. Coverage maps are readily available and can guide attackers to the location of these cables. For example:



Organised cybercriminals could potentially carry out targeted campaigns with the purpose of obtaining knowledge about the precise location of easily accessible fibre.

Bending of fibre

With this method, the cable's coating is peeled down to the protective material covering the fibre itself, enabling the attacker to bend the cable to a point where light can be collected from the cable. If the cable is bent too far, light leaks out of the cable, which can then be collected. Some types of fibre begin leaking light at a bend radius of less than 6.5 to 7.5 centimetres, with the exception of specialised types of fibre.[4] This method can be utilised at a relatively low cost.

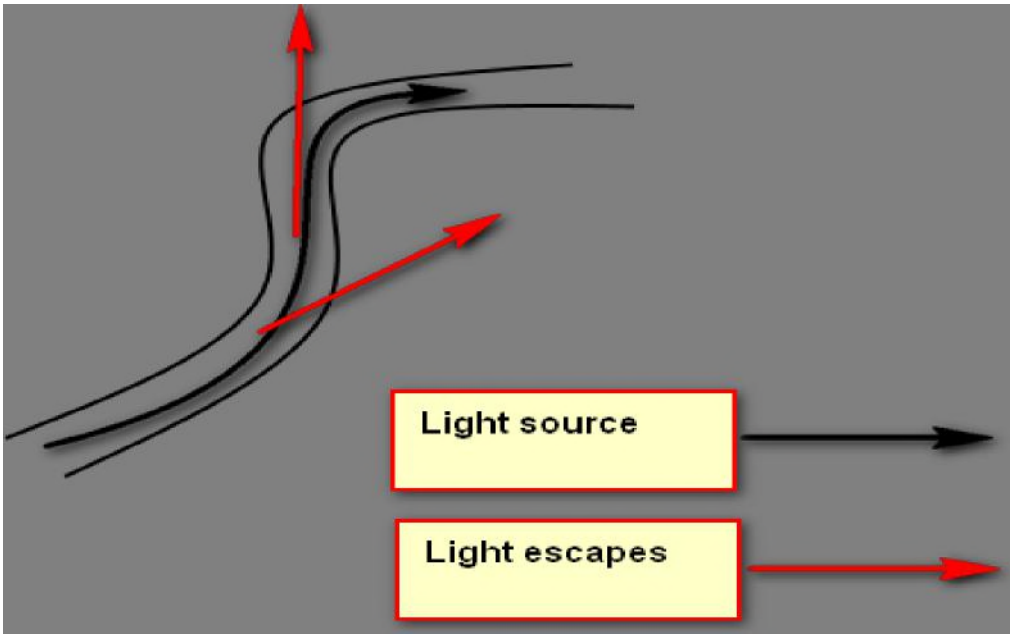


Figure 1 Bent cable

Figure 2 Clip-on Coupler

A bent fibre cable may not be discovered, as it does not result in any loss of signal. Figure 2 shows a mechanism that can bend the fibre and channel the signal in two directions. This type of attack can be performed at multiple locations in the fibre network.

[4] http://fac.ksu.edu.sa/sites/default/files/06149809-OpticalFiberTappingMethodsandPrecautions.pdf
[5] http://fac.ksu.edu.sa/sites/default/files/06149809-Optical Fiber Tapping Methods and Precautions.pdf, https://www.joshruppe.com/fiber-optic-tapping-tapping-setup/

Optical splitting

This method causes some disruption on the line, as the optical cable is split using a clip that cuts into the cable and attaches a second fibre cable, which transmits light from the main fibre to a device controlled by the attacker. However, such an attack may remain undetected for a long time, as the signal is only briefly disrupted when the fibre is clipped.[6] An optical cleaver is no longer reserved for use by large companies, as the technology is now relatively inexpensive. Deloitte therefore views the threat of physical attacks on fibre networks as having increased dramatically in recent years.[7] It should also be noted that the Danish fibre network is comprised of cables laid over a long period of time; not all of these cables have been updated with technologies that make it easier for network operators to detect physical attacks.

Figure 3 Eight-way FBT splitter from China

The following is a scenario involving some social engineering:

"An attacker purchases fibre network provider logos in a large format and sticks them on a rented white/yellow/orange van. The attacker then rents asphalt breaker equipment and digging machinery through a builder's market. Additional equipment investments include a yellow vest with reflectors, a yellow helmet, barricade cones and tape. The attacker then drives out to a location with underground fibre cables and digs down for access. The attacker then attaches the optical splitter and lays fibre optic cable to a secluded location that can be accessed at a later date. The attacker can then return to the site of the connected cable to perform tapping or invest in additional equipment to automatically collect data. "

In this scenario, the attacker would have the capability to intercept all traffic and could therefore eavesdrop on telephone conversations, access non-encrypted MPLS, steal passwords and perform other malicious acts.[8]

[6] http://fac.ksu.edu.sa/sites/default/files/06149809-OpticalFiberTappingMethodsandPrecautions.pdf
[7] https://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-gross-up.pdf
[8] https://www.youtube.com/watch?v=bnzeyBK3kAY

Figure 4 Device for cleaving fibre

Known examples of integrity and confidentiality breaches

There are known examples of the physical installation of tapping devices in fibre networks. These attacks illustrate that fibre networks are not inherently protected against tapping.

The severity of some of these examples also underpins the importance of focusing on the security of data transmitted through fibre cables.

Back in 2000, three of Deutsche Telekom's main trunk lines were successfully attacked at Frankfurt Airport.[9] In 2003, Verizon's fibre network was tapped using an illegally installed device. International events have also revealed that Dutch and German police were the subject of espionage in the form of tapping, as were pharmaceutical companies in England and France.

Additional speculation abounds regarding state-sponsored projects, such as the American submarine "Jimmy Carter", which has allegedly been rebuilt for the purpose of intercepting data transmitted along transatlantic fibre cables.[10]

Current threats and preventive measures

Due to companies' growing demands for bandwidth, new fibre networks are being established faster than ever before and fibre network products are now offered at affordable prices for individuals and companies. Companies today lack insight into the physical and organisational configuration of optical networks. Many fibre network providers do not own the fibre themselves, but rent capacity to provide their services. This means they lack full control over data and its routing through the physical network. For example, some fibre cables may transmit data through other countries, depending on the infrastructure's configuration. The growing supply and volume of installations in private homes and businesses, combined with the declining cost of technology, amount to a high threat of attack on fibre networks. Individuals are now able to make "constructive" changes to their own installations, thus increasing accessibility for potential attackers. Meanwhile, organised cybercrime is a growing industry with extensive technical expertise and financial resources. A range of physical measures can be taken by fibre network operators to detect attempts at the physical or digital tapping of their networks. Digital tapping is already well-known and detection methods are constantly improving, whereas physical detection requires the costly updating of older installations and cables.

The new EU regulation on data protection has brought added focus on the security of data, including data in transit. Companies cannot rely on the ability of network providers to protect data. The customers of these providers are ultimately responsible for the prevention of data leaks.

[9] http://fac.ksu.edu.sa/sites/default/files/06149809-OpticalFiberTappingMethodsandPrecautions.pdf
[10] http://www.thefoa.org/tech/ref/appln/tap-fiber.html

As it is extremely difficult to guard against tapping, not many measures would guarantee the confidentiality and integrity of data transported via fibre networks. Some measures can be taken to monitor the physical integrity of cables, including the use of electrical conductors in the outer coating on cables, which would reveal cable breaches if broken. Another type of fibre cable is available which runs on top of the data-carrying fibre and simply sends monitoring data. Multi-modular fibre installations can monitor any signal alterations that cause modular changes. As mentioned, many of these methods require infrastructural changes often associated with high costs. Furthermore, the network operator is responsible for carrying out these changes.

Fibre network customers do not have many options for securing data confidentiality and integrity. However, Deloitte points to encryption as a method that can be used. Encryption does not protect against the tapping of data traffic itself, but the intercepted traffic will be useless to attackers if strong encryption without vulnerabilities is used.

In the view of Deloitte, the most effective encryption must be used in the protocols closest to the physical transmission. Layer 2 (the network protocol layer, e.g. Optical CDMA, MPLS) can be protected with the use of dedicated hardware devices between end points. This complicates the interception of data to the point that accessing this data would be an incredibly resource-intensive project.

Layer 3 encryption is already available in the form of HTTPS, TILS, etc., but it can be demanding in relation to the devices involved in network transmissions. This is especially true if a large volume of devices is required, as encryption must be uniquely initiated for every single established connection.