

Background Paper Glasfaser-Netzwerke

Risiken und Gefahren bei optischen Datenleitungen

Glasfasernetzwerke sind heute aus der Geschäftswelt nicht mehr wegzudenken. Was aber oft vergessen oder gar verschwiegen wird: Glasfasernetzwerke lassen sich problemlos abhören. Damit stellen sie ein nicht zu unterschätzendes Sicherheitsrisiko dar.



Glasfaserkabel sind Datenleitungen mit bislang konkurrenzlosen Vorteilen. Auf keinem anderen Weg werden derart grosse Informationsmengen schnell und zuverlässig übertragen. Moderne Glasfasernetzwerke werden bei vielen Banken, Versicherungen, Unternehmen und öffentlichen Verwaltungen als Backbone eingesetzt – und ausgerechnet hier sind sie leichte Beute für Wirtschaftsspione. Laut zahlreicher, internationaler Studien haben sich die digitalen Lauschangriffe auf Unternehmen weltweit in den vergangenen zwei Jahren verzehnfacht. Der wirtschaftliche Schaden durch solche Angriffe ist enorm. Das F.B.I. rechnet mit einem jährlichen Schadenspotential durch Wirtschaftsspionage von bis zu 20 Mrd. US Dollar – allein durch technische Attacken innerhalb der Vereinigten Staaten.

1 Glasfaserkabel – das Übertragungsmedium der Zukunft

Glasfasern gewinnen in der Datenübermittlung stark an Bedeutung. Schätzungen weisen auf über 300 Millionen Kilometer gezogene Glasfaserkabel rund um den Erdball. Sie ermöglichen hohe Übertragungsraten und damit besonders leistungsfähige Kommunikationsverbindungen für Daten, Bilder und Sprache. Gigabit-Ethernet ist in Carrier-Netzwerken die Access-Technologie, das Glasfaserkabel das Übertragungsmedium.

Im Geschäftsalltag ist der Informations- und Datentransfer zu einem unverzichtbaren Bestandteil geworden – und zwar in immer grösserem Umfang. Bandbreiten von 1 Gbps und mehr sind für die Verbindung verschiedener Standorte in Städten (MAN), für landesweite Verbindungen (WAN) wie auch für Backup- und Disaster-Recovery-Infrastrukturen (Storage Area Network, SAN) vermehrt an der Tagesordnung. Selbst grosse Datenmengen können auf diese Weise gespiegelt und weit entfernt vom Ort des Geschehens aufbewahrt werden. Spätestens die Terrorattacken auf das World Trade Center haben die Wichtigkeit der Dezentralisierung jedes Daten-Backups vor Augen geführt. Die bedeutenden Vorteile der Glasfaser für solche Netzwerke

(Geschwindigkeit, Kapazität, Wirtschaftlichkeit) haben dazu geführt, dass deren Nachfrage massiv angestiegen ist.

Die verbreitete Wahrnehmung, dass die Glasfaserleitung im Vergleich zum herkömmlichen Kupferkabel besonders sicher sei, stimmt nicht ganz. Denn es gibt verschiedene Möglichkeiten, mit Hilfe so genannter «Optical Tapping»-Methoden Informationen aus Glasfasern zu extrahieren. Das Risiko, dabei bemerkt zu werden, ist gering oder ganz inexistent. Wer nach den benötigten Tools sucht, der findet diese ganz einfach im Internet. Die meisten Telekommunikations-Provider weisen aber immer noch zu wenig auf die wachsende Gefahr hin – oder sind sich dieser gar nicht bewusst.

2 Verletzbarkeit von Glasfaserkabeln

Lauschangriffe auf Glasfaserkabel sind viel einfacher als bislang angenommen. Welche Glasfaser von wem benutzt wird, lässt sich vergleichsweise einfach ermitteln, da einzelne Leitungen eines Kabelbündels zu Wartungszwecken markiert sind. Es genügt somit, die Kabel zu identifizieren, die aus einem Gebäude austreten, um sie an einer frei zugänglichen Stelle anzuzapfen. Allein im Glasfasernetz der Schweiz werden mehrere tausend Verstärker in Kästen gesteckt, die in der Regel nur mit einem Vierkantschlüssel verriegelt sind. Diese Verstärker sind für Unterhaltsarbeiten mit optischen Servicesteckern versehen und bilden so den einfachsten Angriffspunkt in Glasfasernetzwerken.

Grundsätzlich lassen sich alle „optical tapping“ Methoden in drei Gruppen aufteilen:

- Splice-Methoden
- Splitter-/Coupler-Methoden
- Non-touching Methoden

Das Risiko ist real: So entdeckten Geheimdienste in den Vereinigten Staaten illegal angebrachtes Spionage-Equipment innerhalb des Verizon-Fiber-Netzwerks in der Nähe eines Unternehmens – kurz vor dessen Bekanntgabe seiner Quartalszahlen. Die Ermittlungsbehörde vermutet, dass Terroristen ihre Finanzen durch den Aktiengewinn aufbessern wollten.

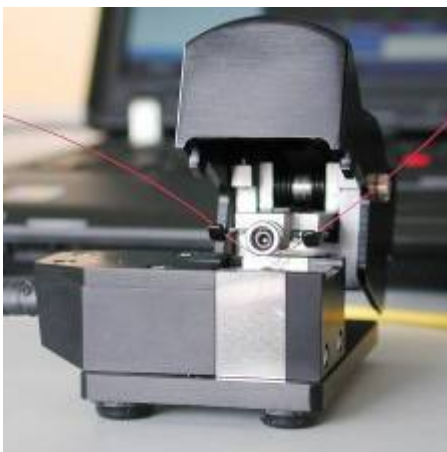
2.1 Optical Tapping - «Splice Methods»



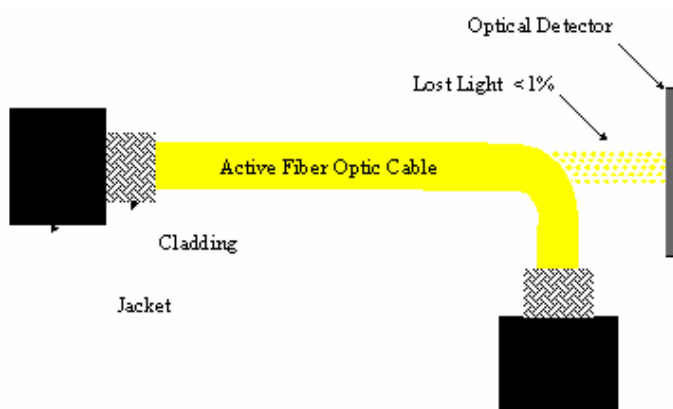
Bei der einfachsten Methode wird die Glasfaser-Strecke aufgetrennt und ein entsprechendes Gerät dazwischen geschaltet. Während der Zeitdauer der Zwischenschaltung ist die Verbindung unterbrochen und dies kann relativ einfach detektiert werden. Wenn die Down-Time allerdings kurz ist, wird kaum ein Provider die Störung untersuchen und die Abhöreinrichtung wird nicht bemerkt.

Bei modernen Abhöreinrichtungen für optische Netzwerke ist es nicht mehr nötig die Verbindung zu unterbrechen und so hat die die «Splicing»-Methode in den letzten Jahren zunehmend an Bedeutung verloren.

2.2 Optical Tapping - «Splitter/Coupler Methods»

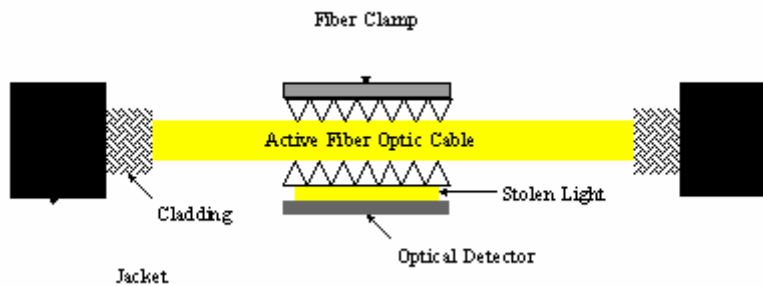


Wird eine Glasfaser gebogen, folgt das durchströmende Licht grösstenteils der Biegung (bending). Ein Teil aber strahlt aus der Faser heraus – wie dies aus dem Physikunterricht hinlänglich bekannt ist. Mit den heutigen, modernen Empfängern genügen schon wenige Prozent des Lichts aufzufangen (schon 1-2% der optischen Leistung reichen aus), um das vollständige Signal zu erhalten und in seine digitale Form zu wandeln. Man kann entweder die ganze Faser mit einer Klemme biegen, die zugleich das Lichtsignal aufnimmt – zum Beispiel mit dem Biegekoppler¹ FCD-10B der kanadischen Firma EXFO.



¹ Bend coupler; Wegen der Reflexionen und der unterschiedlichen Brechzahl zwischen Kernglas und Mantelglas von einer Glasfaser können bei einem gebogenen Lichtwellenleiter nach Entfernen der Beschichtung Strahlen zentrifugal austreten oder aufgefangen werden. Soll die Auskopplung permanent erfolgen, wird die zu biegende Faser und die Anschlussfaser bis auf den Kern abgeschliffen und miteinander verklebt. Auf diese Weise ist auch eine Einkopplung möglich. Dadurch wird die Meinung, Glasfaser seien resistent gegen passive Angriffe, zumindest stark relativiert.

Oder mit mehreren angefügten Dornen einzelne Punkte der Glasfaser so verformen, dass dort Licht austritt.



Das nötige technische Gerät zur Kopplung gehört zur Ausrüstung der Wartungstechniker, die damit den Zustand und die Funktion der Lichtwellenleiter testen – und ist deshalb frei käuflich. Der kanadische Hersteller Canadian Instrumentation & Research, Ltd. etwa bietet das Equipment für rund 1000 US-Dollar im Internet an. Die Signal-Extraktion mittels Biegekoppler ist technisch einfach und problemlos anwendbar, aber aufgrund der unvermeidlichen Dämpfung (bis zu 1dB) grundsätzlich nachweisbar.

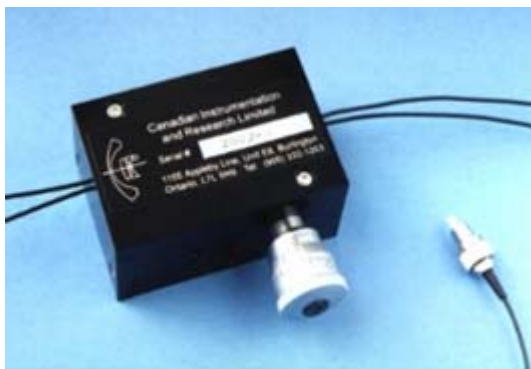


Abb. Polarization Maintaining Variable Ratio Evanescent Wave Coupler, der Canadian Instrumentation & Research, Ltd. eignet sich für Tapping-Attacken auf Singlemode und WDM-Verbindungen unter Ausnützung des so genannten Polarisation-Phenomens.

Grundsätzlich handelt es sich bei der «Coupler»-Methode um eine passive Attacke, allerdings gibt es auch Biegekoppler die für aktive Attacken eingesetzt werden können. Hier geht es nicht primär darum das Lichtsignal zu extrahieren, sondern einen existierenden Informationsfluss mit falschen Informationen (einem Fremdsignal) zu versehen oder zu unterbrechen.

2.3 Optical Tapping – «Non-touching Methods»

Nach dem heutigen Stand der Technik ist ein derart grober Eingriff ins Kabelnetz - wie oben geschildert – überflüssig. Die Deutsche Telekom AG, Bonn selbst hat im Europäischen und Amerikanischen Patentamt eine wesentlich subtilere Methode angemeldet (EP 0 915 356 A1, resp. US 6,265,710 B1). Das Prinzip: Empfindliche Photodetektoren fangen die minimalen Lichtmengen auf, die auf natürliche Weise seitlich aus dem Kabel strahlen. Wegen dieser so genannten Rayleigh-Streuung müssen die Lichtimpulse auf dem Weg durchs Kabelnetz immer wieder verstärkt werden, damit auch bei geografisch weit verteilten Endpunkten ein ausreichend starkes optisches Signal empfangen werden kann. Diese Rayleigh-Streuung lässt sich mittels fokussierenden Elementen auf dem Photodetektor bis zu einer brauchbaren Intensität verstärken oder auf die Eintrittsfläche einer weiteren Glasfaser weiterleiten. Ein Vorteil der Methode - den sich Spione zu Nutzen machen könnten – weder die Leitung noch das Signal wird dabei messbar gedämpft, resp. abgeschwächt. Im Klartext: Die Deutsche Telekom hat mit diesem Verfahren eine Abhörmöglichkeit patentieren lassen, bei der die Glasfaser nicht einmal berührt werden muss – und messbar auch nicht nachweisbar ist (undetected eavesdropping). Auch die «Non-touching» Methode kann als passive oder aktive Attacke ausgeprägt sein.

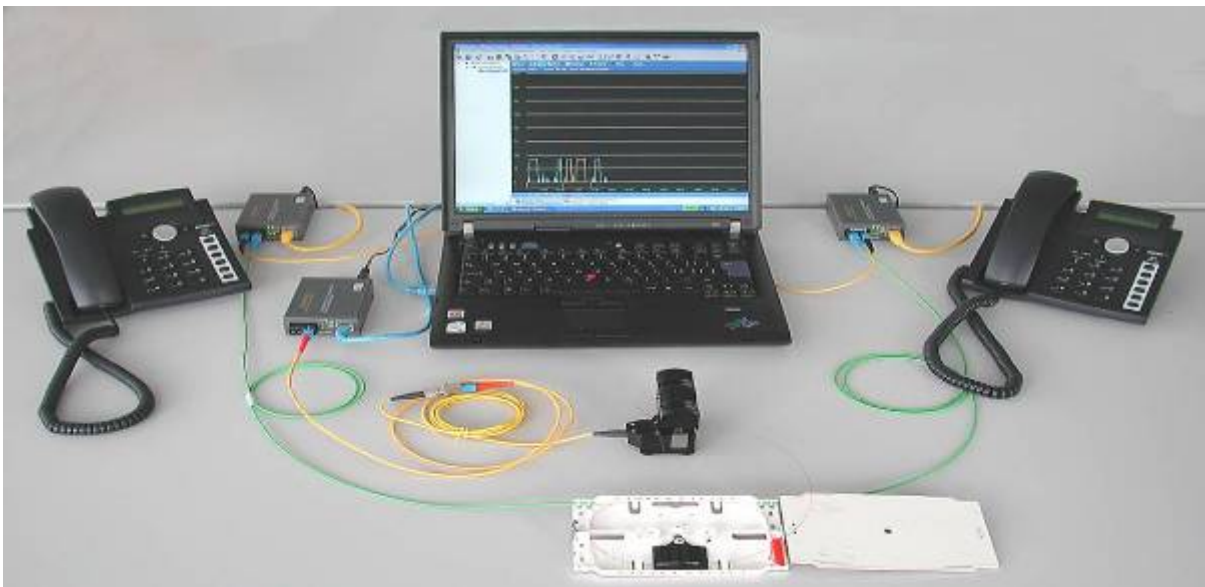


Abb. Testaufbau einer Attacke mit Real-Time Aufzeichnung einer Voice-over-IP Anwendung.

So ist damit der Bericht für das Europäische Parlament zum internationalen Abhörnetz «Echelon» überholt, dass Glasfaserkabel nur an den Endpunkten einer Verbindung angezapft werden könnten.

Basierend auf den Erkenntnissen aus einem internen AT&T-Papier aus dem Jahre 2002 ist ersichtlich, dass das systematische Abhören von Glasfaserkabeln – in den USA z.B. das sehr populäre und von Unternehmen oft genutzte WorldNet – sehr wohl Realität ist. So wurden in diversen Städten der USA im Auftrag der Regierung (unter dem Deckmantel der Terrorismusbekämpfung) so genannte „secret rooms“ aufgebaut um ganz gezielt die Kommunikation zu analysieren. In den angesprochenen Fällen wurden bereits beim Aufbau der Infrastruktur „Splitter“ in die Glasfaserverbindungen eingebaut. Für die Analyse setzt man dabei auf das Produkt „Narus STA-6400“, der gleichnamigen amerikanischen Firma. Im Management dieser Firma ist unter anderem William P. Crowell – ein ehemaliger, erfahrener Mann aus der National Security Agency (1994, als Deputy Director). Herr Crowell gilt als Spezialist für Informationstechnologie, Sicherheit und „Intelligence Systems“ und arbeitete nach seiner NSA-Zeit zuerst als CEO beim amerikanischen Sicherheitsspezialisten Cylink und ist nach deren Übernahme durch die SafeNet im Federal Advisory Board tätig. Seit 9/11 arbeitet er auch in der „Market Foundation Task Force on National Security“ mit und publizierte mehrere Studien zur Thematik der Homeland Security.

2.4 Analyse der extrahierten Daten mittels Packet-Sniffer

Entgegen der verbreiteten Meinung bieten riesige Datenmengen allein keinen Schutz. Um einzelne Informationen aus einer grossen Datenmenge zu extrahieren, reichen bereits entsprechende IP-Nummern oder Schlüsselbegriffe. Anhand der Ziffern lässt sich mit Packet-Sniffer-Programmen die gewünschte Information ganz einfach aus dem Datenstrom herausfiltern und in Echtzeit speichern. Ein Packet-Sniffer ist ein Programm das Netzwerkdaten aufzeichnet, überwacht und analysiert. Des Weiteren kann ein "Sniffer" sowohl legitim als auch illegitim angewandt werden um ganze Netzwerke und auch deren Benutzer zu überwachen. Entsprechende Ablesegeräte und Software sind frei erhältlich.

Ein Beispiel dazu sind die bereits erwähnten Lösungen von Narus mit Hauptsitz in Mountain View, CA (USA). Eigentlich werden solche Lösungen den ISP angeboten, um neue Verrechnungsmodelle für den Datenverkehr zu realisieren. Selbstverständlich können diese Werkzeuge aber auch für die inhaltliche Datenanalyse verwendet werden (ab OSI Layer 3 und höher, inkl. VoIP-Applikationen).

Narus arbeitet auf der technischen Seite mit namhaften Partnern zusammen und liefert Virtual Analyzer Plug-Ins zu fast allen gängigen Netzwerkkomponenten. Aktuell kann die so genannte Internet Business Infrastruktur (IBI) den Datenverkehr bis zu einer Übertragungsgeschwindigkeit von 10Gbps, resp. OC192 analysieren. Als Kunden führt Narus auf ihrer eigenen Webseite u.a. folgende Telekommunikations-unternehmen aus: AT&T, Brasil Telecom, Korea Telecom, KDDI, Telecom Egypt, Saudi Telecom, France Telecom, T-Mobile und U.S. Cellular.

3 Schutzmassnahmen

Überwachen lässt sich die gesamte Fiber-Infrastruktur kaum. Wie gravierend die Sicherheitslücke ist, lässt sich jedoch schwer abschätzen. Während Netzausrüster und Netzbetreiber hierzulande lediglich ein hypothetisches Risiko sehen, bewertet der grösste nordamerikanische Industrieverband Association of Manufacturers (NAM) den «optischen Datenklau» als reale Gefahr. Bei der NAM mutmasst man sogar, dass das Anzapfen von Glasfaserleitungen eine weit verbreitete Methode der Wirtschaftsspionage sei. Nach Auskunft des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) sind Glasfaserübertragungswege tatsächlich nicht abhörsicher. Daher sei die Datenverschlüsselung äusserst wichtig. Rechtliche Vorschriften gibt es allerdings nur für die Rüstungsindustrie, nicht aber für Unternehmen und Behörden mit ihren Datenleitungen in ausgelagerte Rechenzentren.

3.1 Chiffrierung – die Sicherheitslösung für Glasfasernetzwerke

Wenn Daten in optischen Fiber-Netzwerken unterwegs sind, befinden sich fast immer sensitive Informationen darunter – das ist auch bei Finanzinstituten, Versicherungen, Pharma-, Chemie- und Industrieunternehmen sowie bei öffentlichen Verwaltungen oftmals der Fall. Sind Integrität, Vertraulichkeit und Authentizität dieser Informationen nicht absolut garantiert, entsteht für den Benutzer dieser Technologie ein möglicherweise existenzielles Risiko. Die einzig sinnvolle und garantiert sichere Massnahme, sich vor jeglichen Angriffen zu schützen, ist das Verschlüsseln der Informationen beim Übergang in das öffentliche Netzwerk mit speziellen Hochleistungsverschlüsselungslösungen.

3.2 Gigabit Ethernet Verschlüsselung

InfoGuard AG bietet eine neue Sicherheitslösung «EtherGuard1», resp. «EtherGuard10». Sie basieren auf dem erfolgreichen und bewährten Konzept, welche bei namhaften Banken und führenden Unternehmen erfolgreich eingesetzt wird und sich als «Best Practice» etabliert hat.



Das System chiffriert auf OSI-Layer 2 und bietet so 100%-Datendurchsatz bis auf eine Übertragungsgeschwindigkeit von 1 & 10Gbps und arbeitet im Netzwerk vollkommen transparent und protokollunabhängig. Die maximale Performance (100% Verschlüsselungsdurchsatz) sowie die extrem

kleine Latenzzeit (<5us) ermöglichen den Einsatz der Geräte auch bei zeitkritischen

Anwendungen und stark ausgelasteten Links. Die Verschlüsselungsgeräte bieten absolute Abhörsicherheit bei Punkt-zu-Punkt Verbindungen, seien dies in Form von Dark Fibers oder in gemultiplexten Topologien mit CWDM/DWDM.

Die Sicherheit basiert auf einer einzigartigen Sicherheitsarchitektur und erfüllt höchste Anforderungen, wie sie in hoch sensitiven Umgebungen gestellt werden. So wurden unsere Sicherheitslösungen nach den Vorgaben der Common Criteria entwickelt. Für die Verschlüsselung der Daten wird der starke, öffentliche Advanced Encryption Standard (AES) mit einer Schlüssellänge von 256 Bit oder 128 Bit verwendet.

Die EtherGuard-Produkte sind explizit auf Langzeitbetrieb ausgelegt und benötigen praktisch keinen Unterhalt. Für die Übertragung der Daten über das Glasfasernetzwerk werden handelsübliche Transceiver der Bauform SFP oder XFP verwendet, welche für unterschiedlichste Distanzen und Wellenlängen verfügbar sind.

Als Schweizer Unternehmen stehen wir für höchste Qualität bei unseren Produkten und absolute Unabhängigkeit bei der Implementierung unserer Sicherheitsfunktionen ein. So wurden alle sicherheitsrelevanten Module durch unsere ausgewiesenen Sicherheitsspezialisten in der Schweiz entwickelt und produziert.

Quellennachweis:

FCW.com, "Lights out", 12. Juni 2006, Brian Robinson

Securitysolutions.com, „Hacking at the Speed of Light“, 1. April 2006, Sandra Kay Miller

Virgo Publishing, "Big Brother Is Watching", 3. Januar 2006, Charlotte Wolter

"AT&T Deploys Government Spy Gear on WorldNet Network", 16. Januar 2004

Computerworld, „Intelligence ops in Baghdad show need for security back home“, 8. April 2003, Dan Verton

Wolf Report, „Das Schweigekartell I & II“, März 2003, Wolfgang Müller-Scholz

White Paper on Optical Taps, 9. Februar 2003, Oyster Optics, Inc.

Frankfurter Rundschau, „Glasfaser mit Durchblick“, 4. September 2002, Herr Gábor Papp

Frankfurter Allgemeine Zeitung, „Hört, hört - Wie einfach Glasfasern angezapft werden können“, 13. März 2003, Herr Heinz Stüwe

Die Welt, „Glasfaserkabel sind nicht abhörsicher“, 3. Februar 2002, Herr Gábor Papp

White Paper on Optical Taps, 1. August 2002, Oyster Optics, Inc.

United States Patent, US 6,265,710 B1, 24. Juli 2001, Deutsche Telekom AG

Europäisches Parlament, Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation, 11. Juli 2001

Europäische Patentanmeldung, EP 0 915 356 A1, 18. September 1998, Deutsche Telekom AG