

THREATS TO FIBER- OPTIC INFRASTRUCTURES



*A BLACKHAT FEDERAL BRIEFING
1-2 OCTOBER, 2003*

- **Introduction to Fiber Network Infrastructure Technology**
- **Threats**
- **Tapping [A Demo]**
- **Defending Fiber Infrastructures**
- **Physical Security Defenses**
- **Conclusion**
- **Q&A**

Your Presenters

- **Mark Gross** [Opterna]

- Vice President
- mgross@epix.net
- www.opterna.com

- **Robert J. Bagnall** [iDEFENSE]

- Dir, Intel Ops
- rbagnall@idefense.com
- www.idefense.com



Perceptions

- Item

–*Washington Technology, April 10, 2003*

“Running a continuous strand of fiber also assures that a fiber optic line has not been tapped into—a bonus of security conscious agencies.”



Threats



Opterna

For Enlightened Networks™

- ComputerWorld – April 2003

“Tapping fiber optic cable without being detected, and making sense of the information you collect, certainly isn’t trivial, but has been done...for the past seven or eight years.”

Gartner Group

Intrusion

Eavesdropping

- Phone
- Fax
- Video teleconference

Injection

- Data Integrity Attacks

1. Eavesdropping Case Study

- The Wolf Report – March 2003

“Security forces in the US discovered an illegally installed fiber eavesdropping device in Verizon’s optical network. It was placed at a mutual fund company...shortly before the release of their quarterly numbers.”

- Baghdad – April 6, 2003 - Fox News

2. Injection Case Study

- FAA

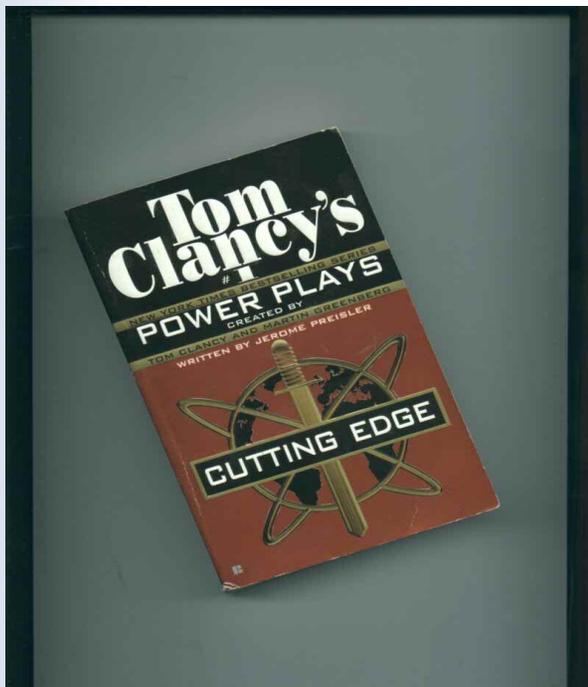
Assessing the Security Threat

- TV show "Alias"- fall, 2002-3rd episode
 - Item
 - CIA agent Sidney Bristow is sent off on a mission with a device that will be used to tap SD-6's fiber optic cable



Assessing the Security Threat

- Tom Clancy's new book, "Cutting Edge", March-2003

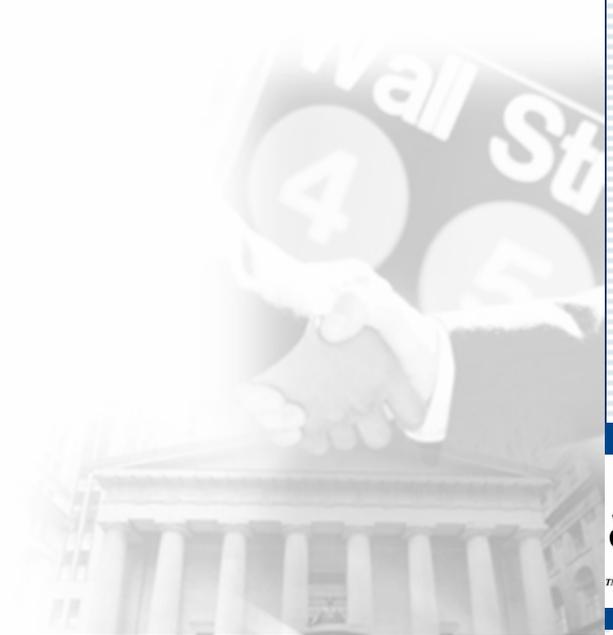


-Premise is that a submarine fiber optic cable will be tapped and the information mined for a profit

Assessing the Security Threat

The concept and practice of tapping secretly into a fiber optic cable, wherever it is, has become part of the lexicon- a standard mode of operation, to be discussed and considered as a legitimate method to gather information.

Introduction to Fiber Network Infrastructure Technology



US Fiber Facts

- There are over 90 million miles of single-mode fiber in the US alone
- Only 25% is currently “lit”
- 90% of the installation has occurred since 1996
- Technology advances increase data transport capacity on fiber exponentially on an annual basis

US Fiber Facts

- FO networks form the backbone of the US communications infrastructure
- Recent technology advances have resulted the ability to easily and inexpensively tap an FO cable
- US military, intelligence, law enforcement, and financial services information run on fiber, and are thus exposed

Fiber: The Basics

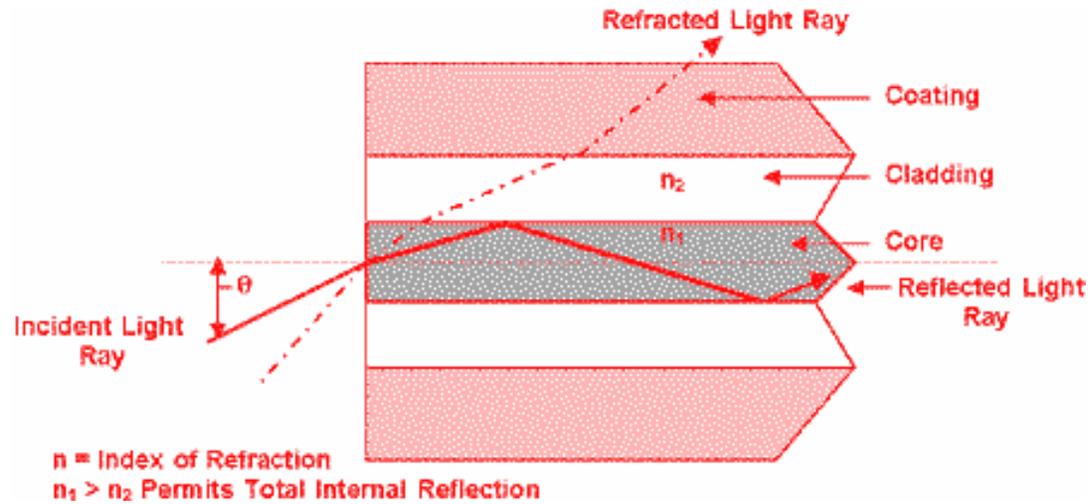
- Multimode
- Single mode
- Electrical-Optical Conversion



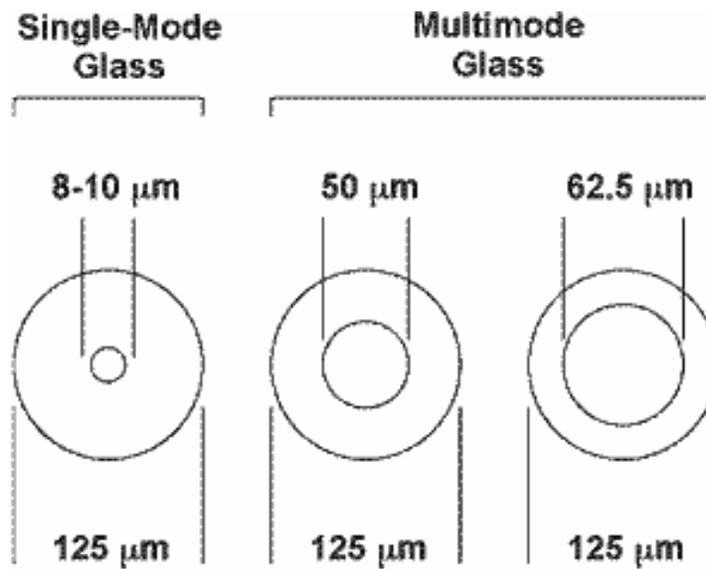
Opterna

For Enlightened Networks™

Structure of a Fiber Optic Cable

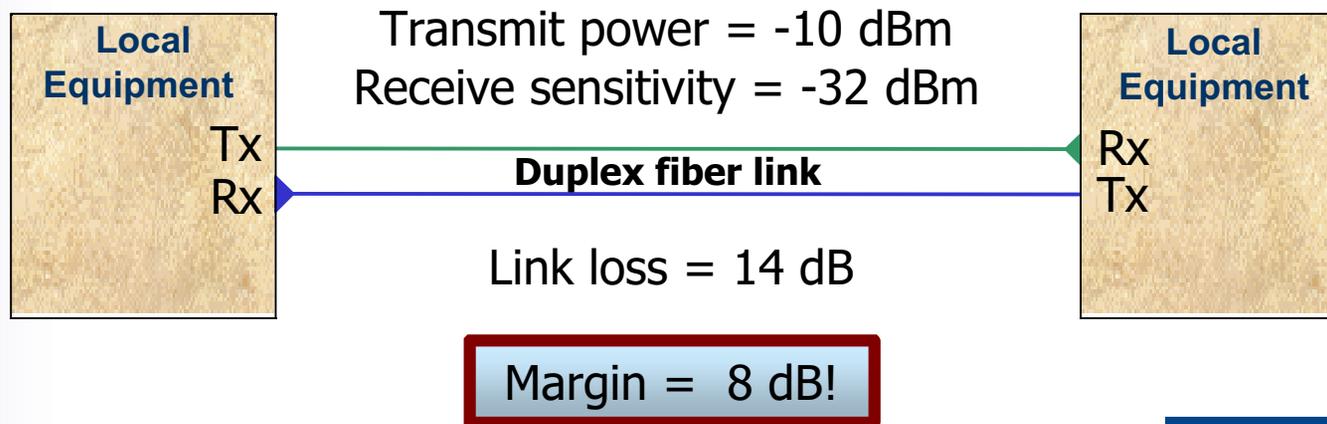


Structure of a Fiber Optic Cable



Assessing The Security Threat

By design, optical systems have wide optical budgets. A well designed fiber link can experience a wide variety of optical anomalies with no data loss, bit errors, signal failures, or network warnings whatsoever.



Threats

- ComputerWorld – April 2003
 - “Fiber optic cables...can be easily intercepted, interpreted, and manipulated using standard off-the-shelf equipment that can be obtained legally throughout the world. More important, the vast majority of public fiber networks do not incorporate methods for detecting optical taps, offering an intruder a relatively safe way to conduct corporate espionage.”

Tapping

[The Basics]



Active Fiber Tapping

- WSJ – May 2001

“...former intelligence officials confirmed that NSA technicians used a special submarine to tap into a fiber-optic cable on the seafloor in the mid-1990s, around the same time that fiber amplifiers began displacing electro-optic amplifiers. The sub supposedly had a special compartment into which the cable could be hauled, enabling technicians to install the tap.”

- IEEE – June 2003

“Further evidence of the NSA’s ability to tap undersea fiber-optic cables – and its intention to go on doing it – is a \$1B project at Electric Boat in Groton, Connecticut, to outfit a new Navy submarine, the USS Jimmy Carter, with a special 45-meter-long section. The Navy has never disclosed the exact purpose of the expensive addition to the \$2.4B sub, but most observers...believe it is to tap undersea fiber-optic cables.”

The Tap

It has been shown that an intruder can easily tap a fiber line without being detected through the use of a low-cost "Clip-on Coupler"



The Tap

Commercially available taps are readily available that produce an insertion loss of 3 dB which cost less than \$1000!



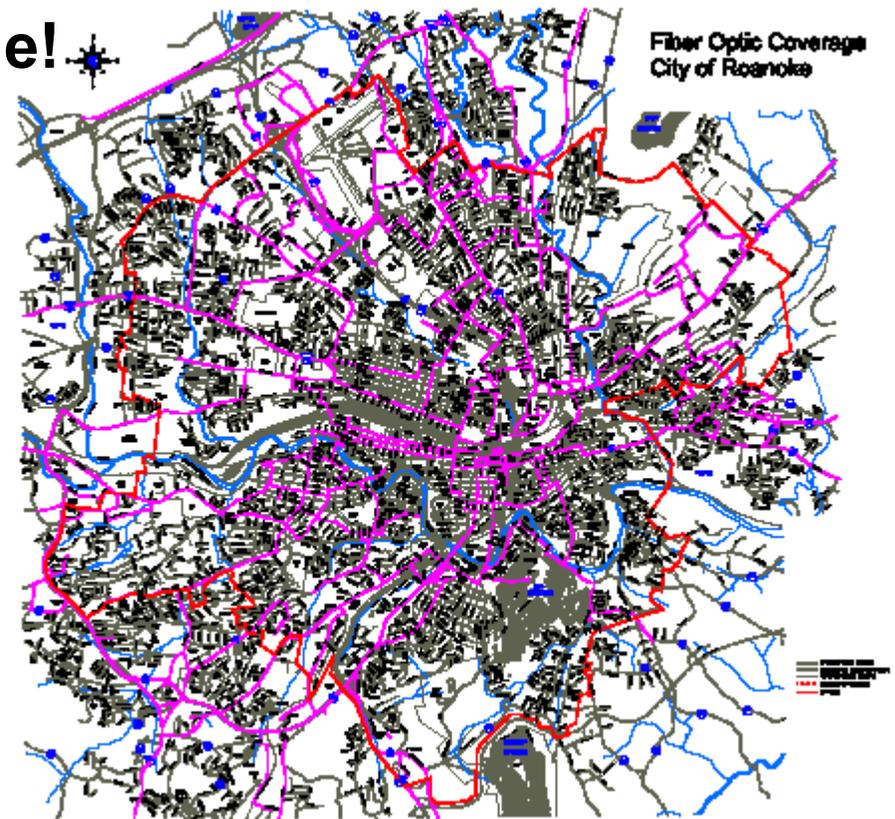
Taps currently in use by state-sponsored military and intelligence organizations have insertion losses as low as 0.5 dB!

Security Threat - Disclosure

Too Much Information Online!

Efficiency over Security

Social Engineering & End-User Awareness



Opterna

For Enlightened Networks™

Security Threat - Actors

- Adversarial nation states [N. Korea]
 - Intercepted comms of US military build-up activities
- International Espionage [France]
 - Targeted US high-tech, scientific, & pharmaceutical corporations
- Corporate Espionage [US-vs-US Company]
 - MCI targeting Verizon for brand damage [tap disclosures]
- Rogue Groups [Al-Qaeda]
 - Intercepting network traffic between US & embassies
- Rogue Individuals [Miscreants, Hackers]
 - Wire transfer & other financial attacks

Security Threat – PnP & Ops

- Companies do not view themselves as a CIP asset
- Basic security policies not in place or followed
- Procedures not enforced
- Lack of awareness/education for end-users
- Lack of accountability of end-users after training

Defending Fiber Optic Infrastructures



Defenses

-  Provide continuous, real-time, protocol independent, physical layer monitoring of the fiber network connection
-  Identify optical anomalies by analyzing the optical carrier
-  Built-in Route Protection Switching proactively enhances network integrity by auto-switching to pre-configured backup paths as required.

Physical Security of Fiber

- 1> DETECT the event
 - monitor both primary and backup paths

- 2> ISOLATE the affected path
 - within the first few milliseconds

- 3> RE-ROUTE traffic using the RPS

- 4> Notify the management system



Physical Security of Fiber

- Physical Layer Intrusion Prevention Systems: desired traits

Automatically identifies, differentiates, and characterizes 8 distinct optical event types:

- Intrusions
 - Optical Signal Injections & Eavesdropping
- Cable Breaks
- Transients
- Receiver Overloads
- Low Optical Signal Levels
- Data Signal Loss
- Identify Causes of Power-off Conditions

Physical Security of Fiber

- **Functionality:**

Monitoring the optical carrier...

- *DOES NOT* decode the data on the optical carrier
- Is a *PASSIVE* system
- Data remains in the optical state and is not regenerated

Physical Security Measures



Bury the fiber in concrete



Weld shut or secure manhole covers, wiring closet doors, riser access panels, & elevator shafts



Use of OTDR Technology:

- No continuous monitoring
- No intrusion shutdown
- No characterization or optical faults detected
- Ineffective at detecting dynamic or transient disturbances



Optical Power Level Attenuation Monitoring

- No intrusion shutdown
- No fault characterization



Opterna

For Enlightened Networks™

Physical Security Measures



Vibration Sensing Technology

- No intrusion shutdown
- 6 dB optical insertion loss
- *FiberSenSys*



Phase modulation of the optical signal

- *Oyster Optics*



Real-time fiber carrier monitoring systems

- *FiberSentinel*



Opterna

For Enlightened Networks™

Conclusion



Security Concerns

- Tapping [easy & cheap]
 - Injection & Eavesdropping
- DoS Attacks
- Physical Security & Access
- Environmental & Man-made DoS Events



Desired Security Elements

- Continuous Real-time Monitoring
- Capability to Differentiate & Characterize Optical Anomalies
- Automatic Intrusion Detection Shutdown
- Automatic Re-route to Redundant Paths

Questions





How to Contact Us

Mark Gross, VP [Opterna]

mgross@epix.net

www.opterna.com

Robert J. Bagnall [iDEFENSE]

Dir, Intel Ops

rbagnall@idefense.com

www.idefense.com



Opterna

For Enlightened Networks™