Vulnerability of Fiber Optic Infrastructure to Intrusion

Assessing the Security Threat

- There exists today between 83 and 90 ***Million*** miles of single mode fiber installed in the United States (Business Week, August 2001)
- Only 25% of that fiber is currently lit
- 90% of this fiber has been installed since 1996
- Because of technology advances (e.g.:WDM), the data transport capacity of this fiber increases dramatically almost on an annual basis

Assessing the Security Threat

- Item
  - *Wall Street Journal Online -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.”

Assessing the Security Threat

- Item
  - *IEEE Spectrum Online – June 1st, 2003*
    - "Further evidence of the NSA's ability to tap undersea fiber-optic cables--and its intention to go on doing it--is a $1 billion project at Electric Boat, Groton, Conn., 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 $2.4 billion sub, but most observers, including Pike, believe it is to tap undersea fiber-optic cables."

Assessing the Security Threat

- Item
  - *"Tapping a 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"*

    John Pescatore

    Gartner Group analyst, former NSA analyst

    (Computerworld, April 2003)

Assessing the Security Threat

- Item
  - *“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.”*

    Computerworld, April 2003

Assessing the Security Threat

- Item
  - *"At the beginning of 2000 the Supervisory Board of Deutsche Telekom was busy with the security of the high tech network at Frankfurt Airport after culprits gained access to the three main fiber trunk lines"*

Wolf Report

March, 2003

Assessing the Security Threat

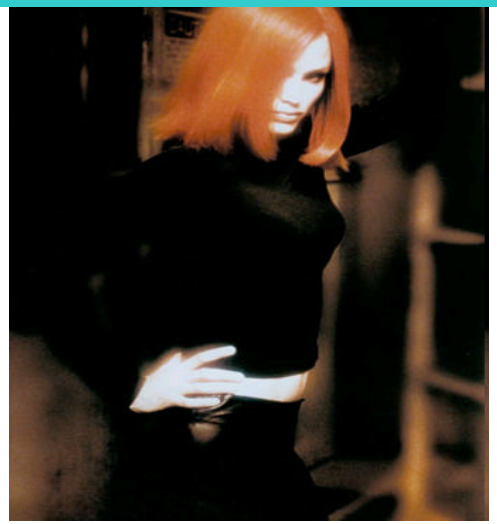
- Item
  - *"Security forces in the US discovered an illegally installed fiber eavesdropping device in Verizon's optical network. It was placed at a mutual fund company.....shortly before the release of their quarterly numbers"*

    Wolf Report

    March, 2003

Assessing the Security Threat

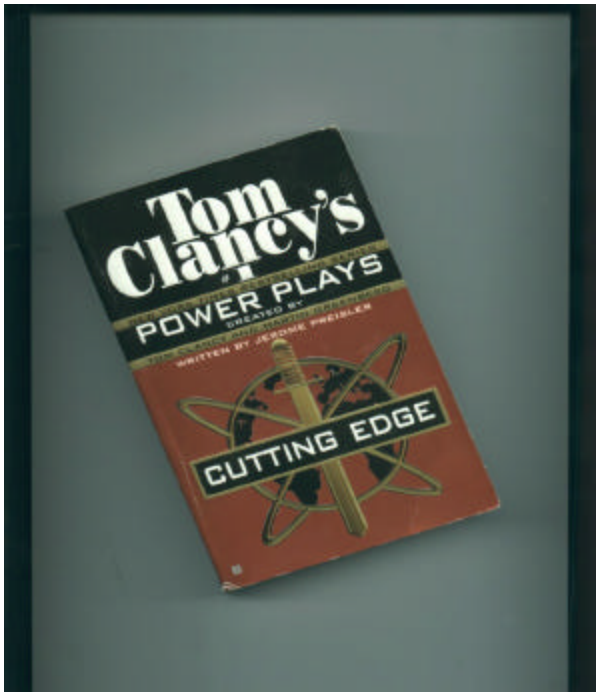
- TV show “Alias”- fall, 2002-3rd episode
  - *Item*
    - CIA agent Sidney Bristow is sent off on a mission with a device that will be used to tap SD-6’s fiber optic cable



Opterna
For Enlightened Networks™

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

Opterna
For Enlightened Networks™

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.

Assessing the Security Threat

- 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. “

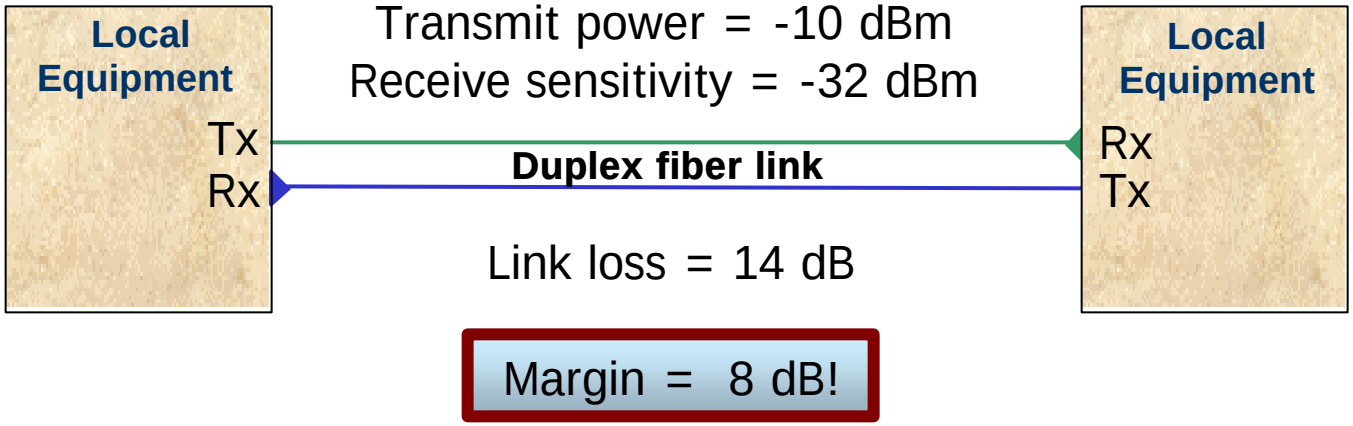
Fiber Optic Security Threat

- *Fiber optic networks form the backbone of our communications infrastructure*
- *Recent technology advances have resulted in the ability to easily and inexpensively tap a fiber optic cable*
- *Our most secret and confidential information is now exposed to those wishing us harm*
- *Our nations military, intelligence, law enforcement, and financial institution information is now vulnerable*

Opterna
For Enlightened Networks™

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.



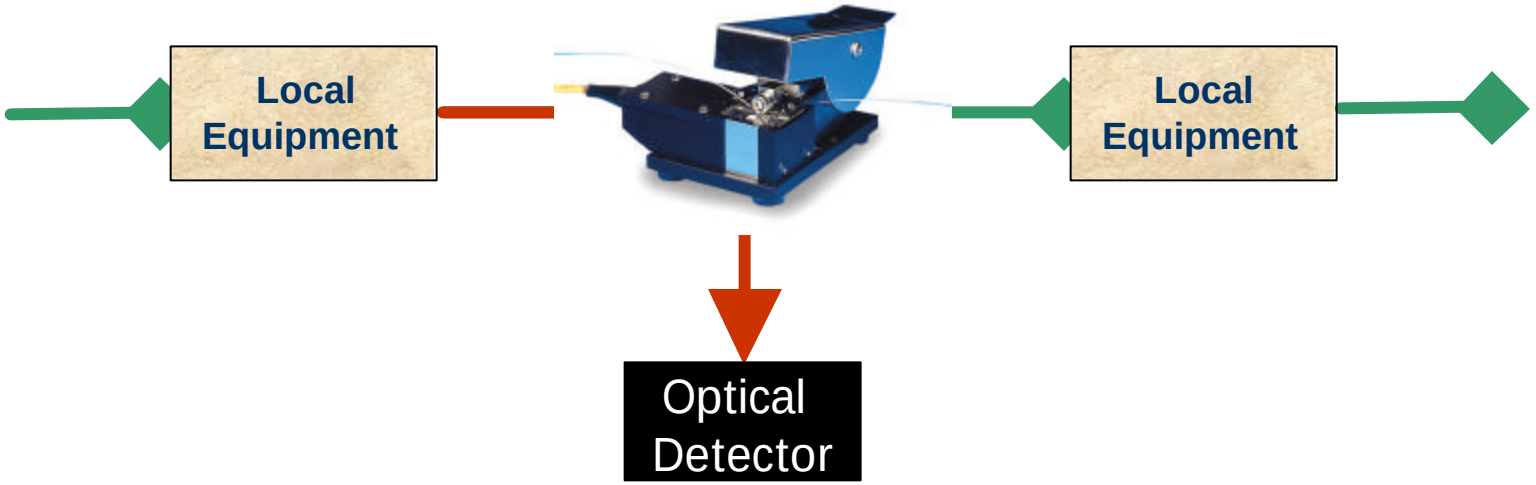
Opterna
For Enlightened Networks™

Assessing the Security Threat

Optical communication systems are designed to ignore changes below the margin!

Assessing the Security Threat

It has been shown that an intruder can easily tap a fiber without being detected by using a low cost "clip-on coupler"



Opterna
For Enlightened Networks™

Assessing the Security Threat

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

Assessing the Security Threat

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

Properties of a Physical Layer Intrusion Prevention System

- *Provide continuous, real-time, protocol independent, physical layer monitoring of a fiber optic network connection*
- *Identify optical anomalies by analyzing the optical carrier*
- *Built in Route Protection Switch works proactively to enhance network integrity by switching to a backup path as required*

Opterna
For Enlightened Networks™

Physical Layer Security Device Functionality

- ***Detect*** the event
  - *Both primary and backup paths are fully monitored*
- ***Isolate*** *the affected path (in milliseconds)*
- ***Re-route*** traffic to the backup fiber path

  (Optical "route protection switch")
- ***Notify*** the management system

Opterna
For Enlightened Networks™

Desirable Properties of a Physical Layer Intrusion Prevention System

- *Automatically identifies, differentiates, and characterizes eight distinct optical event types*
  - *Intrusions*
  - *Optical signal injection by an intruder*
  - *Cable breaks*
  - *Transients*
  - *Receiver overloads*
  - *Low optical signal levels*
  - *Loss of data signal*
  - *Identify local or remote power off conditions*

Opterna
For Enlightened Networks™

Physical Layer Security Device Functionality

- Monitoring the optical carrier
  - **Does not** decode the data on the optical carrier
  - System is passive
    - data remains in the optical state and is not regenerated

Opterna
For Enlightened Networks™

Physical Layer Security Technologies

- Bury the fiber in concrete
- Weld the manhole covers, wiring closet doors, riser access panels, elevator shafts *shut*
- *OTDR* technology
  - *No continuous monitoring, no intrusion shutdown, no characterization of optical faults detected, ineffective at detecting dynamic or transient disturbances*
- Optical power level attenuation monitoring
  - *No intrusion shutdown and no characterization of faults*
- Vibration sensing technology
  - *No intrusion shutdown and 6dB optical insertion loss*
  - *FiberSenSys*

Opterna
For Enlightened Networks™

Physical Layer Security Technologies

- Phase modulation of the optical signal (scrambling)
  - *Oyster Optics*
- Real-time fiber carrier monitoring systems
  - *FiberSentinel*

Desired Elements

- *Continuous, real-time monitoring*
- *Differentiate & characterize optical anomalies*
- *Automatic intrusion shutdown (if desired)*
- *Automatically re-route traffic to an alternate fiber path*

Opterna
For Enlightened Networks™