ENHANCING THE DEPLOYMENT AND SECURITY OF SIPRNET AND JWICS NETWORKS USING INTRINSIC FIBER MONITORING

Shane Shaneman
CSC
Clarksburg, MD

and

Cary Murphy
Network Integrity Systems, Inc
Conover, NC

ABSTRACT

With the increased requirements for SIPRNET and JWICS access, secure network connectivity has become increasingly pervasive throughout the Department of Defense. The increased deployment of secure networks has resulted in an evolution of secure network architectures and the Information Assurance methods and tools used to protect them. Specifically, new technological advances in the ability to monitor and protect fiber optic cables and connections possess huge potential for cost savings and enhanced protection of critical networks and C4ISR facilities.

With the accelerated development and deployment of C4ISR applications on the Global Information Grid, warfighters are developing a strategic dependence upon the availability and integrity of secure networks. While encryption has been used for decades to protect the confidentiality and non-repudiation of national security information (NSI), encryption alone provides no coverage or protection against threats to network availability and integrity. Through recent developments in intrinsic fiber monitoring technology, critical connections can now be proactively monitored to detect any threats or physical attacks on the network WITHOUT degrading network performance or restricting network bandwidth.

Using the principles of the Defense in Depth strategy, intrinsic fiber monitoring provides a very agile and scalable protection methodology that can be used by itself or in combination with cryptographic equipment to provide the required protection of classified networks and the ability to withstand the ever-increasing threats to the networks.

THE SIPRNET EXPLOSION

Over the last few years, secure network deployments have become much more pervasive, and frequent due to
(1) the availability of actionable, classified information,
(2) the development and increased utilization of advanced C4ISR applications, and
(3) the warfighter's need to achieve and sustain information superiority.

With access to secure networks becoming more and more ubiquitous, new building construction and renovation activities must now address not only the long-term performance and scalability of the voice and data network being installed – but also its ability to support and protect secure network access and multiple-classification networks over the life-cycle of the building without requiring extensive re-cabling or worksite disruption. Even if a building today has no requirement to provide the warfighter access to SIPRNET or JWICS network(s), the potential for future requirements (and future tenants) has to be considered in order to minimize Total Cost of Ownership.

EVOLUTION OF SECURE NETWORK ARCHITECTURES

Historically, secure network deployments have been very limited in size and scope, and very isolated from mainstream Local Area Network requirements or deployments. Typically, secure network deployments were limited to a very small workcenter or Sensitive Compartmented Information Facility (SCIF) (with the obvious exception of facilities fulfilling the Intelligence, Surveillance, and Reconnaissance (ISR) mission). Due to the limited scope and density of the deployment, the predominant network architecture utilized to provide secure connectivity was the Home Run architecture. The Home Run architecture is characterized by several disparate, independent cables being installed from the Red/Black Equipment Area or Closet to each workstation.

1-4244-1513-06/07/$25.00 ©2007

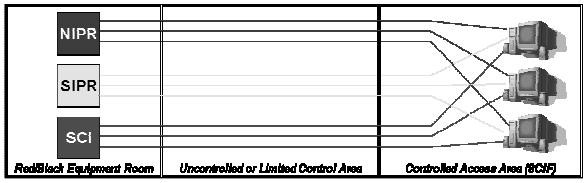


Figure 1 The Home Run Architecture

The Home Run architecture's simplistic approach made it the architecture-of-choice for single-drop and low-density secure network deployments. However, with the accelerated deployment of SIPRNET and JWICS networks that we are seeing today, deployments have become much broader and more pervasive – rendering the 'Home Run' architecture too cumbersome and complicated. Furthermore, over the last 3-5 years, fiber optic cables have rapidly replaced the use of copper cables for secure network connectivity. For these reasons, secure network architectures have evolved to utilize more of a Zone Architecture.

The Zone Architecture is typically characterized by a single or few high-fiber-count optical trunk cables deployed to a zone box or consolidation point within the workcenter or area requiring secure connectivity. This DRASTICALLY reduces the number of cables installed, and that also will have to be protected. From the Zone Box, patchcords can be installed and easily routed to each workstation. (Since the Zone Box or consolidation point is typically located inside of a secure area, the cabling from the zone box to the workstation would require much less hardening or protection.) By utilizing the Zone Architecture, secure connectivity can easily be scaled from a medium- to a large-deployment as well.

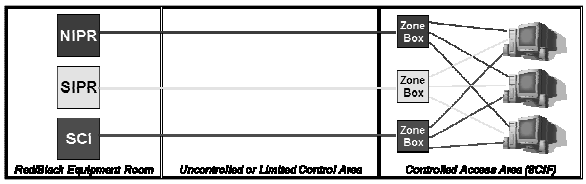


Figure 2 The Zone Architecture

As a result of the secure network architecture evolution, there are fewer cables to protect and an overwhelming majority of the zone trunk cables installed are fiber optic cables. Both of these significant changes are direct enablers for the use of Alarmed Carrier technology using intrinsic fiber monitoring to provide enhanced protection for the secure networks.

ALARMED CARRIER TECHNOLOGY

For over a decade, Protected Distribution Systems (PDS) as specified by the Committee on National Security Systems (NSTISSI 7003) have provided physical hardening and protection of secure networks. According to the NSTISSI 7003 guidelines, a PDS system can be used in lieu of encrypting national security information, or as a means to provide enhanced protection for the availability and integrity of the network. A PDS can take the form of either a hardened carrier (i.e. cables installed in EMT or in a concrete-encased duct bank) or an alarmed carrier (i.e. cables that are alarmed or installed inside of an alarmed carrier such as a pressurized conduit.)

While alarmed carrier PDS has been an approved option for many years, it has been used in only a minor fraction of the secure network deployments to date. This is due in part to the complexity of the secure network architectures being utilized (i.e. Home Run, copper cables, etc), but even more so due to the complexity and low effectiveness of the legacy alarmed carrier equipment being utilized. The first type of alarmed carrier deployed utilized pressurized cables and conduits to 'detect' an intrusion in the system - which would cause a loss of pressure in the conduit. Unfortunately, this system worked extremely well in the laboratory environment – but was next to impossible to maintain and operate in the real world. Small leaks and pin holes created a never ending chain of false alarms and maintenance that totally eroded the users confidence in system's reliability and the resulting level of protection.

In the 1990's, perimeter defense equipment manufacturers began to use fiber optic cables deployed along a wall or fence line to monitor and detect intrusions. The fiber optic cable would 'sense' vibrations or disturbances in the fence and cause an alarm to be generated. Through the technology transfer of these traditional fence line systems, a few companies began to use these 'sensing' fibers as part of an alarmed carrier system – where the sensitive fiber optic cable would be installed inside of a metallic carrier (i.e. EMT) along with the national security system cables that required protection – essentially using EXTRINSIC fiber monitoring to provide protection to any cables installed in the same carrier as the sensing fiber. Typically using interferometric or modalmetric technology, these vibration sensors monitor for mechanical breaching of the pipe, for instance with equipment such as a saw, as a prelude to an intrusion. In theory, the sensing fiber would detect any vibrations or disturbances caused by tampering or attempted intrusion into the metallic carrier and generate an alarm. However, the environment that the technology was transferred into (i.e. inside of a building) was vastly different from that where it was previously utilized. As a result, the system eventually

suffered from some of the same performance and reliability concerns that plagued pressurized conduit systems.

INTRINSIC FIBER MONITORING DEVELOPMENT

In 1993, Rome Laboratory worked closely with Hughes Network Systems to develop a Fiber Alarm Modem that INTRINSICALLY monitored individual strands of fiber for any disturbances or anomalies that could be indicative of tampering or attempts to 'tap' the network. The system evolved and was officially adopted by the Committee on National Security Systems as the IDOCS system – Intrusion Detection of Optical Communication Systems (NSTISSI 3015). The benefit of the IDOCS system over other alarmed carrier technology is that (1) it was monitoring the same fiber or cable that required protection, and (2) its COMSEC-specific development negated the false alarm issue that would result from the technology transfer of traditional fence line systems. While the IDOCS system received great fanfare from the COMSEC community, its high costs and low speeds limited its adoption. From 1993-2001, intrinsic fiber monitoring received little to no attention or technology development, relegating alarmed carrier deployments to use extrinsic fiber monitoring – capturing a very small niche of the overall PDS deployments.

With the increased deployment of fiber optic cables in Local Area Networks in the 2001-2003 timeframe, intrinsic fiber monitoring finally re-emerged thanks to technology development and advances such as wave-division multiplexing, etc. A few equipment manufacturers began to develop intrinsic fiber monitoring technology that could protect ALL of the optical fibers inside of a cable simply by monitoring for anomalies or disturbances on as few as one or two fibers within the fiber optic cable (up to 288-fibers). Rather than monitor an external sensor fiber, intrinsic systems alarm fibers within the cable. These alarmed fibers can be unused, or "dark" fiber monitoring, or they can be fibers currently or intended to be carrying data, or "active" monitoring. Another key benefit of intrinsic fiber monitoring is scalability of protection. By using fibers inside of the cable that requires protection, additional fibers can be incrementally monitored in order to provide increasing protection to the network… all the way to alarming every fiber.

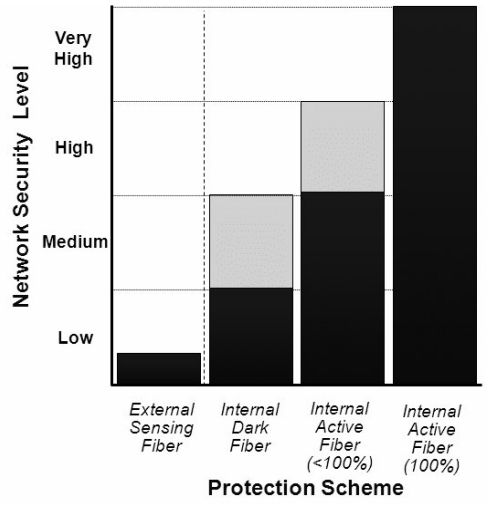


Figure 3 Network Security Protection Levels

INTRINSIC VS. EXTRINSIC FIBER MONITORING

As there is nothing inherent with intrinsic monitoring that would require motion sensing rather than vibration sensing, the unique nature of monitoring an actual data fiber allows some freedom in technology. Typical latest generation intrinsic monitoring systems implement a motion sensing system, often modal metric or polarization based; these are designed to alarm upon minute degrees of motion. In contrast, extrinsic systems, by virtue of the physical separation from the protected cable, are often optimized for vibration sensing. This creates non-insignificant challenges of differentiating actual intrusions from such things as vibrations caused by passing traffic, or HVAC air handlers. With respect to extrinsic fiber monitoring, efforts to minimize false alarms can potentially result in a lack of sensitivity to those intrusions. The focus on vibration sensing also leads to a potential vulnerability with extrinsic monitoring. Studies have shown some success in the use of vibration dampening materials applied to the conduits as a means to impede detection. This only exacerbates the sensitivity tradeoff within an installation in which resistance to false alarming is paramount, and sensitivity is at a minimum.

The primary difference between extrinsic versus intrinsic monitoring is (1) what is being monitored, and (2) what is being detected. Extrinsic fiber monitoring is optimized for monitoring the physical stability of a metallic carrier (which contains National Security System cables) via a sensitive fiber optic cable and detecting any vibration or potential breach of the carrier. Intrinsic fiber monitoring monitors the actual data fiber within the National Security System cable(s) and detects any movement or disturbance of the fiber optic cable.

A key concern with extrinsic fiber monitoring is the ability of a an attacker to either (1) breach the metallic carrier without detection, or (2) to be able to separate what is being monitored (the sensitive fiber optic cable) from what needs to be protected (the National Security System cables). While traditional attempts to breach a metallic carrier (i.e. hacksaw, drill, rotary cutter, etc.) would generate significant vibration, recent testing has proven that the use of vibration dampening material can SIGNIFICANTLY degrade the ability of extrinsic fiber monitoring to detect ANY breach of the metallic carrier. As the chart below illustrates, extrinsic fiber monitoring is extremely limited on its ability to provide multiple levels of protection, and potential detection once the metallic carrier is successfully breached. In comparison, intrinsic fiber monitoring offers maximum protection at ALL levels.

Table 1 Graduated Levels of Protection

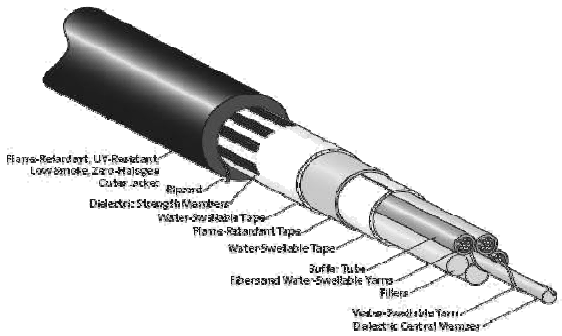
	Extrinsic	Intrinsic
Cable	Yes	Yes
Sub-tube	No	Yes
Active Fiber	No	Yes
Adjacent Fiber	No	Yes

QUANTITATIVE RED TEAM TESTING

While extrinsic monitoring is used to protect against access to a cable, intrinsic monitoring goes further and protects against tampering and penetration. To illustrate the various levels of graduated protection, and the effectiveness of intrinsic monitoring through each stage of a cable attack, intrusion testing was performed on a standard communication grade optical cable with intrinsic fiber monitoring on only 2 out of the total 48-fibers. In order to test each level of protection, multiple sub-unit tubes were attacked and penetrated, and both alarmed and non-alarmed fibers were tapped (using a Laser Precision AM-450 macro-bend coupling device):

RED TEAM TEST OVERVIEW

I. Cable Tested:
Corning Altos® All-Dielectric Gel-Free Cable
4 Tubes of 12x 250µ SM
Corning p/n 048EW4-T4101D20



ALTOS LSZH Gel-Free Cable | Drawing ZA-1887

II. Intrinsic Fiber Monitoring Equipment
Interceptor™ Fiber Security System

III. Test Configuration
The fiber optic cable was monitored by an intrinsic monitoring system that alarmed one fiber
in one sub-tube, additionally 1km of fiber was connected at each end of the link under test in
order to simulate an actual installation. each end of the link under test in
order to simulate an actual installation.

IV. Test Procedure:
- Breach cable jacket to access sub tubes
- Breach unprotected sub-tube in order to access fibers
- Breach protected sub-tube in order to access fibers.

Figure 4 Red Team Testing Overview

Red Team Results:
Each step of the intrusion process caused alarms as denoted in the table below:

Table 2 Red Team Testing Results

Test Procedure Step	# of Alarms
Breaching and removing the outer jacket and accessing the inner tubes	26 Alarms
Breaching a sub-unit WITH an alarmed fiber and tapping a non-alarmed fiber	+20 Alarms
Breaching a sub-unit WITHOUT an alarmed fiber and tapping a fiber	+10 Alarms

The chart below helps visualize the ability of intrinsic fiber monitoring to detect tampering and intrusion AT MULTIPLE STEPS in the process, and to provide consistent protection to the cables being tested REGARDLESS of the location of the alarmed fiber in the sub-unit or cable. For this test, the fiber monitoring equipment was first autoconfigured per manufacturer's instructions. To rule out random or spurious false alarms, it then sat undisturbed for 90 minutes prior to intrusion testing while being monitored for false alarms. Absence of false alarms was confirmed.

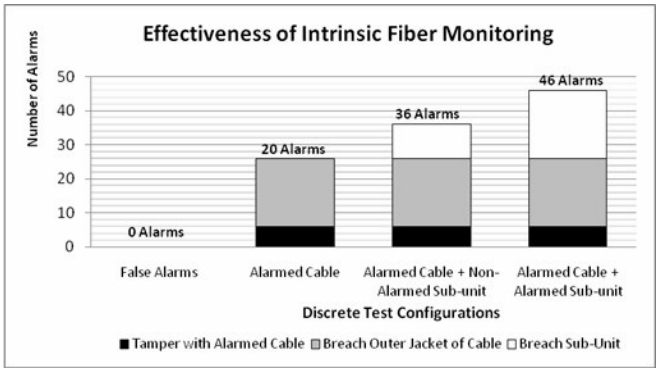


Figure 5 Effectiveness of Intrinsic Fiber Monitoring

The significance of these results is that intrinsic fiber monitoring provides comprehensive and reliable protection of fiber optic cables with consistent, repetitive alarms at multiple stages throughout each Red Team test configuration. Furthermore, due to the ability of intrinsic fiber monitoring equipment to auto-configure the monitoring parameters and baseline to the specific environment around the infrastructure to be protected, false alarms were virtually non-existent. In comparison with user feedback on the long-term performance of extrinsic fiber monitoring, the quantitative results on intrinsic fiber monitoring represent a drastic improvement in both the end user confidence and the level of protection provided to National Security Systems.

ENHANCING NIPRNET→SIPRNET MIGRATION

In addition to increased protection, Intrinsic Fiber Monitoring also offers significant cost savings over traditional PDS installations. In a recent deployment by CENTCOM, an alarmed carrier deployment using intrinsic fiber monitoring was able to save more than $500k over concrete-encasement and encryption on a single building connection. Intrinsic fiber monitoring also supports the utilization of existing infrastructure to provide SIPRNET connections on an as-needed basis versus the need to install totally new infrastructure when using extrinsic fiber monitoring. The increased deployment of fiber optic Zone architectures is also a prime enabler for alarmed carrier deployment using intrinsic fiber monitoring as the fiber optic trunk cables can be readily protected – providing effective protection up to the zone box or consolidation point with the ability to scale secure connectivity on as as-needed basis (as well as enabling the installation of the fiber optic cables ABOVE the ceiling and negating the daily visual inspections required for traditional hardened carrier EMT installations.

PROTECTION AGAINST ADVANCED THREATS

By utilizing intrinsic fiber monitoring, each individual fibers carrying TS/SCI or Special Access program (SAP) information can be monitored to provide the ultimate in protection against the advanced threats identified below:

1) Data Theft or Repudiation of Information- While fiber optics are immune to electromagnetic and radio frequency interference, and also negate concerns around compromising emanations, it is still possible for a skilled attacker to 'tap' a fiber. There are three widely known methods for extracting or injecting data mid-span in an optical fiber: bend coupler, evanescent coupling[1], and Rayleigh scattering[2].

2) Denial of Service Attacks- There are two primary types of physical denial of service threats to fiber optic infrastructure with the end-goal of degrading the availability and integrity of the network.

a. Signal Interruption- Optical transmission is interrupted by breaking or blocking the optical path. This is typically accomplished through tampering

with the cable, cutting the fiber, or unplugging connectors.

b. Signal Injection- With this attack, an optical signal, typically of similar wavelength to the data signal, is injected and launched into the fiber. The intention is to saturate the data receiver with a signal level beyond its operating region, causing it to effectively go blind.

CONCLUSION

With C4ISR networks becoming more pervasive and more and more of a combat-enabler, protecting the strategic networks and the classified information that they carry is a critical focus for the DoD. Advances in intrinsic fiber monitoring, specifically for alarmed carrier PDS deployments, provides a robust new solution for Information Assurance and network security that provides agile, scalable protection of secure fiber optic networks such as SIPRNET and JWICS. In comparison with previous alarmed carrier technologies, intrinsic fiber monitoring provides more reliable and consistent protection – with the ability to scale protection to meet increasing threats, higher classification of information, or dynamic requirements. Finally, with Alarmed Carrier PDS deployment fully authorized in NSTISSI 7003, federal agencies and DoD services can leverage intrinsic fiber monitoring equipment TODAY for enhanced protection of C4ISR networks and a *very* cost-effective alternative to encryption and hardened carrier PDS deployments (i.e. EMT, concrete encasement, etc.).

ACKNOWLEDGEMENTS

The authors wish to thank Joseph Giovannini and Mark Bridges of Network Integrity Systems for input into the content of this paper, and for the cable testing described herein.

REFERENCES

1) M. Failes, "Optical Contact Evanescent Wave Fiber Optic Coupler," U.S. Patent 4,688,882, Aug 25, 1987.

2) H. Walter, "Method and Device for Extracting Signals Out of a Glass Fiber," U.S. Patent 6,265,710, July 24, 2001.