PANDUIT®

Managing Physical Security Risk in Physical Layer Infrastructure Solutions

Protecting Against Network Intrusion Using Keyed Connectivity Systems

WHITE PAPER

Introduction

Industries including government, finance, and education have a need for heightened security beyond conventional software-based solutions. With user access requirements ranging from a simple TCP/IP Internet connection to immediate access to the most secure, high-bandwidth network at the facility, many organizations require their data networks to be separated at the physical layer to help control user access and mitigate the risk of unauthorized connections.

The challenge to maintain security and manage risk along all connection points is becoming a top priority for network stakeholders. Each point of connection within a network represents a risk for a potential security breach and must be safeguarded against intruders, both purposeful and accidental. This requires tight security controls to protect sensitive data running over multiple data systems and networks.

This paper describes how keyed connectivity systems as part of a Unified Physical Infrastructure[SM] (UPI) solution mitigate risk across the physical infrastructure by enhancing secure network strategies. These systems work by controlling access to discrete connections at the user level (i.e., the link between workstation and outlet) and preventing inadvertent cross-network patching by technicians and/or unauthorized users. The paper presents the security drivers responsible for the adoption of keyed solutions, and then demonstrates how multiple and precise mechanical keying features on connectors make keyed connectivity the optimal solution for secure infrastructure deployment.

Key Government Policies and Mandates

Effective implementation of e-government initiatives is critical to achieving responsive, efficient, and cost-effective government. Several policies and guidance documents published by the U.S. Government during the past decade have increased adoption of new technologies, including fiber optic and keyed connectivity systems for environments with multiple networks:

- **Clinger-Cohen Act of 1996.** This act has become the main driver for adoption of new information technologies in the U.S. Government. The act states that the government will adopt best practices from the commercial world, improve acquisition of information technology, and deploy IT broadly to improve productivity, efficiency, and effectiveness of federal programs and services.
- **E-Government Act of 2002.** This act mandates that government expand the use of the Internet and computer resources to provide more government services online (such as filing taxes).
- **Security Technical Implementation Guides (STIGs).** These guides are published by the U.S. Defense Information Systems Agency (DISA) to provide additional technical guidance for standardized secure installation and maintenance of information technology products within government facilities and offices.

Mindful of these mandates and guidance resources, the government developed a strategy known as “Information Assurance” (IA). The Information Assurance program is comprised of strategies designed to protect networks from unauthorized access; to detect intrusions when and where they occur; to identify intent of intrusion; and to counteract threats and maximize threat responses.

Network Separation Strategies Support Information Assurance Initiatives

One strategy to support Information Assurance is to separate discrete data networks at the physical layer to enhance both network flexibility and security. The need for flexibility arises from the wide variety of network users in secure facilities. At one time, users would have included only the people who worked in (or were employed by) the facility. Increasingly, network users at a facility routinely include visitors, employees of third-party organizations who are momentary users, and staff members moving about the facility.

Authorized friendly users naturally expect unimpeded access to their resident network; at the same time network administrators must manage risk and prevent unauthorized connections from occurring, whether accidental or purposeful. The separation of networks at the physical level (as opposed to electronic or software security levels) supports security initiatives in the following ways:

- Employees of different departments can work securely at the same government facility, accessing only those networks to which they are entitled. These could be extensions of their proprietary corporate or agency networks, securely coexisting side-by-side but separately.
- Separation of multiple networks can also prevent access by third party vendors and contractors who, through their design or engagement in servicing the network, could potentially become viable security threats.
- Visitor and guest access can be authorized based on role or rank in the organization. No matter where they are located during their visit, these users can be provided access to only the networks for which they are rightful and authorized users.
- Specific networks are more difficult to identify in a separated network environment, which can discourage hackers, terrorists, and other adversaries seeking to gather intelligence, deny network service to others, corrupt a network, or simply embarrass the host organization.

The National Security Agency (NSA), in a public outreach to business and academia as well as other units of government, publishes information from its National Information Assurance Research Laboratory (http://www.nsa.gov/niarl/index.cfm). A useful white paper that briefs the reader on the range of threats to data network users is also available from the following Web site (http://www.nsa.gov/snac/support/defenseindepth.pdf).

Meeting Demand for Security at the Physical Layer

For organizations that require very tight security controls over sensitive data running over multiple data networks and systems, it can be a challenge to maintain security along all points. Each connection point presents a risk for a security breach that must be managed and guarded. Both copper and fiber connectivity designs and architectures have been developed to overcome these challenges and meet growing network security demands.

Fiber to the Desktop (FTTD) is one of the architectures of choice for deploying multiple secure networks to the workstation (see Figure 1). The high bandwidth and small form factor of fiber optic cabling enable the flexible deployment of complex, sophisticated, and demanding applications that support modernization and consolidation efforts. Fiber cables can extend for long distances with minimal loss of signal integrity, from hundreds of meters to tens of kilometers.

Fiber media is also intrinsically difficult to tap. The signal carried by fiber is not affected or altered by nearby radio frequency or electro-magnetic transmissions: no radio or electro-magnetic signals are accidentally emitted from fiber optic cabling, nor can a signal be stolen by positioning listening equipment near the fiber cable. The signal can be tapped only by directly cutting the cable, an act that can be readily detected.

Shielded copper cabling is an alternative media choice for secure applications. Foil and/or braided shielding within the cable prevent signals from coupling between cables and provide superior immunity to Electromagnetic Interference and Radio Frequency Interference (EMI/RFI), making it extremely difficult for unauthorized users to listen in.

Users should weigh factors such as media reach as well as the cost, availability, and power consumption of active equipment to determine which media best fits their application. For example, the reach and bandwidth of fiber optic technologies may be required to carry signals across long distances. For enterprises and government agencies that use copper in workstation areas, shielded twisted pair (STP) solutions offer a higher level of security than unshielded twisted pair (UTP) solutions.

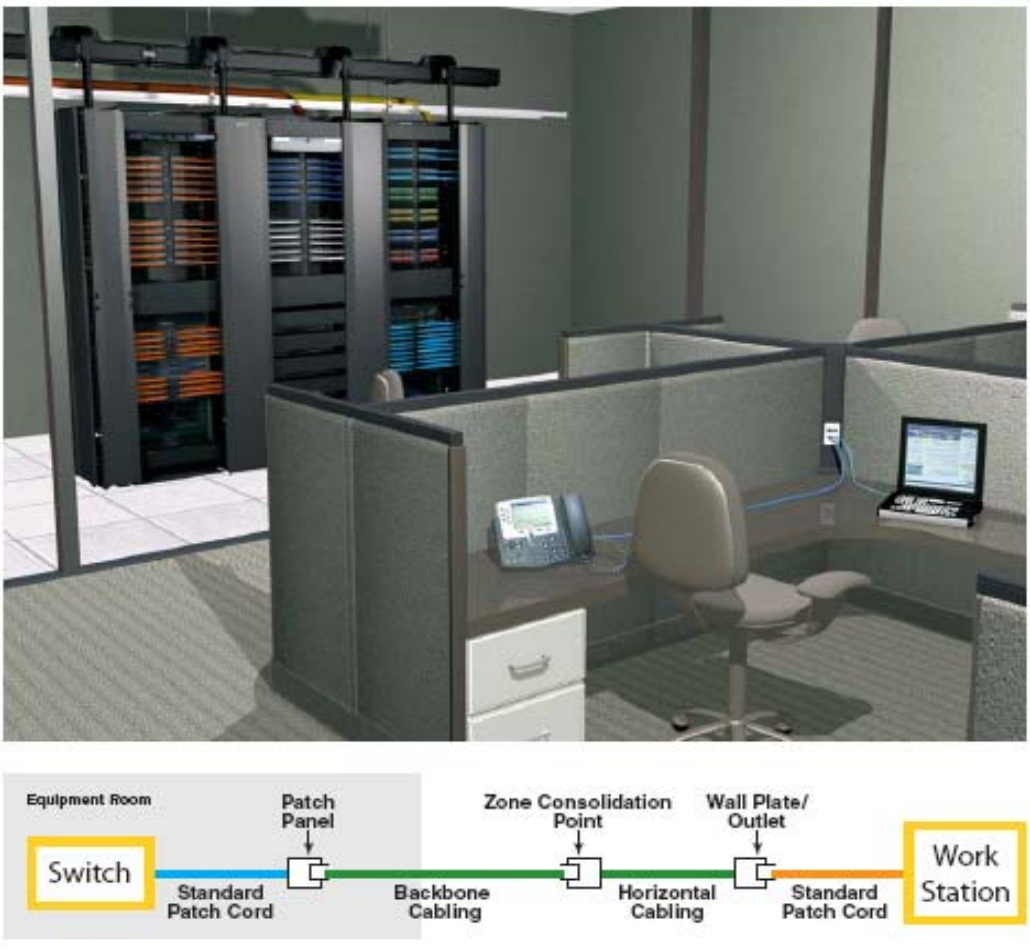

Figure 1. In FTTD applications multiple points of connection exist along the fiber optic channel, from the data center or main equipment room to the desktop.

Benefits of Keyed Connectivity Systems

Fiber and copper keyed connectivity systems are comprised of all necessary elements (connectors, adapters, patch cords) to deploy a physically secure network infrastructure. These systems employ specialized connectors and adapters that physically prevent access to all but the network for which a user is authorized. The idea is similar to requiring a key to unlock a door.

Color-Coded, Mechanical Keying Functionality

Color-coding ensures visual separation of networks by visually distinguishing connections for user convenience (see Figure 2). Network managers assign each discrete network its own color, and only connectivity of that color may be used across the channel from outlets and wall plates to zone enclosures and consolidation points.

Positive and negative keying features on each connector match only with corresponding features on similarly colored adapters and/or patch cords. Unwanted connections are prevented by the unique mechanical geometry associated with connectors for each color, keeping multiple networks separate and secure throughout the facility.

These combined features provide true keying security by:

- Limiting network access to specific functional key types
- Preventing the insertion of other keyed and non-keyed connector products that would compromise the secured keyed network
- Ensuring that only authorized personnel perform moves, adds, and changes to the network

Figure 2. Color-coding visually distinguishes discrete networks to help prevent unauthorized connections at the outlet (shown here) and elsewhere across the channel.

Quick Verification of Secure Network Separation

Keyed connectivity systems provide secure data networks with quick visual verification of secure network separation at all points across the channel. These systems ensure that different personnel cannot plug into each other's networks, preventing not only a compromise of mission but also a compromise of established physical layer security protocols.

The availability of several keyed networks throughout a facility enables resident staff as well as visitors to move about the facility freely with the ability to visually identify and then access the appropriate network. At a military installation, for instance, two users with differing levels of security clearance and/or network access can work on separate projects without overlap or loss of data security.

Also, for installers and similar network technicians working in dense patch field areas, the color-coding on keyed connectivity systems makes it easy to identify correct ports for fast and easy MACs and troubleshooting. The separation in the physical layer does not impinge on software-based security such as login, password, MAC registration, and other software security systems. With best-in-class keyed systems, the chance that a well-meaning user will successfully connect to the wrong network is greatly minimized.

PANDUIT Keyed LC System Provides Best Value

The *PANDUIT* Keyed LC System uses a modular system of proprietary connector and adapter products to support end-to-end separation of co-existing fiber optic data networks. Innovative keyed system components are available to connect all fiber cabling elements in an enterprise running from the main equipment room to the desk, delivering best value to organizations seeking to increase security and minimize risk.

Other keyed systems in the marketplace have been defeated by permitting an alien connector – either a differently keyed (or non-keyed) connector from the same manufacturer, or another manufacturer's connector – to be substantially inserted into a keyed port. This can result in a complete optical connection and thus compromise network security. In contrast, the *PANDUIT* Keyed LC System is tamper resistant and robust against intrusion, securing networks against any other connector except the appropriate matching and color-coded *PANDUIT* keyed connector.

PANDUIT Keyed LC cable assembly, adapter and quick-termination connector components all feature both positive (key) and negative (keyway) elements that mechanically distinguish connections (see Figure 3) to maximize network security. This combination of keys and keyways results in up to 18 different keying options, allowing a high number of discrete and secure networks to coexist in the same facility while preventing all un-alike keyed connectors and adapter ports from mating.

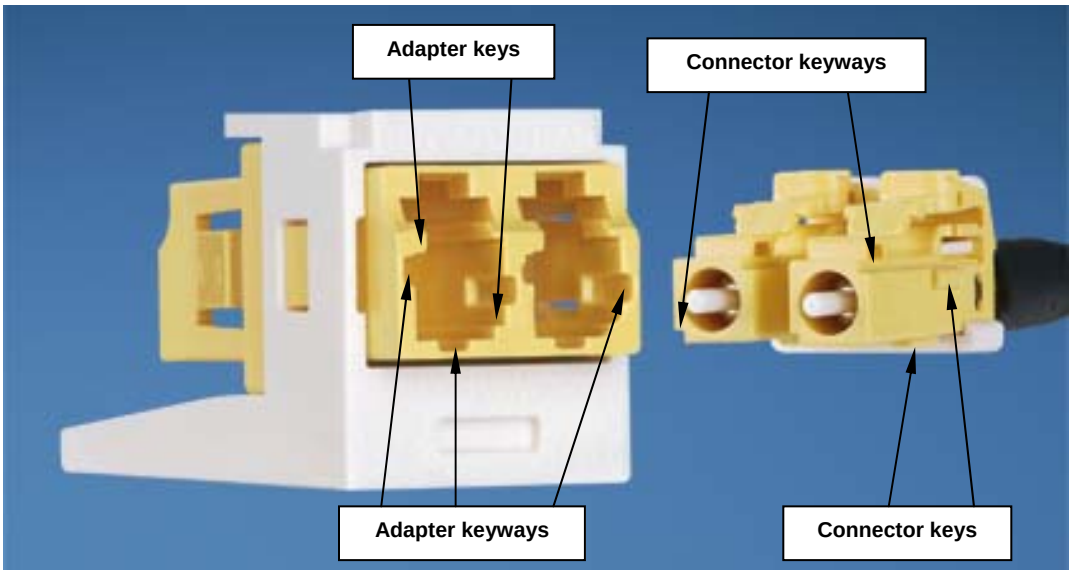

Figure 3. The *PANDUIT* Keyed LC System provides a superior level of security because its system of both *keys* and *keyways* prevents un-alike keyed *PANDUIT* connectors, as well as other manufacturers' connectors, from being inserted into a *PANDUIT* Keyed LC Adapter port.

Unique *PANDUIT* connector lock-in and adapter blockout devices provide added security by securing a connector into its port and blocking out connections to selected ports (see Figure 4). The lock-in duplex clip for the cable assembly connector prevents adapter latches from disengaging from the connector unless an installation/removal tool is used. The tool also enables blockout devices to be snapped in or out of LC adapters or receptacles. These tools are available from *PANDUIT* to limit installation or removal of lock-in and blockout devices to only authorized users.

Conclusion

Maintaining security and managing risk across multiple discrete networks can be challenging, as each connection point along the channel represents a potential security breach. Keyed connectivity systems deliver a proven level of network security combined with installation convenience. By using keyed connectivity, network designers can provide secure, controlled network access to authorized users, and network stakeholders can easily ensure effective network separation throughout their facility.

Color coding on each connector and adapter pair visually differentiates keys, and robust key and keyway features prevent unauthorized user connections and cross-network patching errors from occurring across network connection points. The availability of end-to-end keyed components, the number of color-coded key options, and lock-in and blockout devices provide heightened security and high-performance installations required by today's secure networks. The *PANDUIT* Keyed Connectivity System is part of a portfolio of products that mitigate physical security risk in the infrastructure and enable agility throughout the organization.

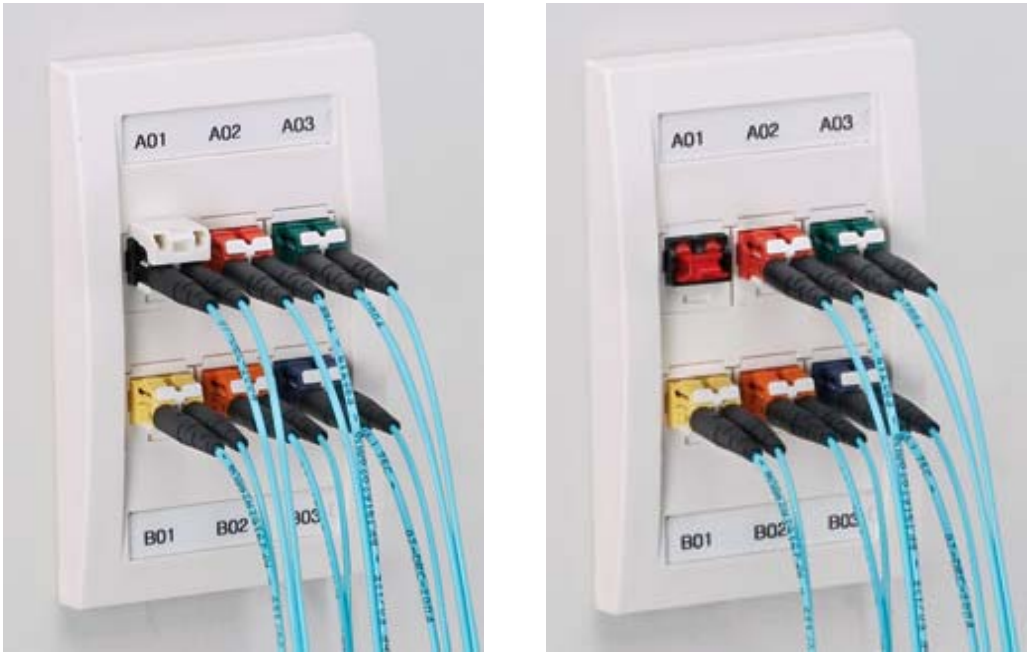

Figure 4. Lock-In (left) and Blockout (right) devices further prevent unintentional moves, adds, and changes to *PANDUIT* Keyed LC deployments, mitigating the risk of connectors becoming accidentally dislodged or otherwise compromised.

About *PANDUIT*

PANDUIT is a world-class developer and provider of leading-edge solutions that help customers optimize the physical infrastructure through simplification, increased agility and operational efficiency. *PANDUIT*'s Unified Physical Infrastructure (UPI) based solutions give Enterprises the capabilities to connect, manage and automate communications, computing, power, control and security systems for a smarter, unified business foundation. *PANDUIT* provides flexible, end-to-end solutions tailored by application and industry to drive performance, operational and financial advantages. *PANDUIT*'s global manufacturing, logistics, and e-commerce capabilities along with a global network of distribution partners help customers reduce supply chain risk. Strong technology relationships with industry leading systems vendors and an engaged partner ecosystem of consultants, integrators and contractors together with its global staff and unmatched service and support make *PANDUIT* a valuable and trusted partner.

www.panduit.com · cs@panduit.com · 800-777-3300