500 Business Center Drive Pittsburgh, PA 15205 USA
412.494.2800   CAGE 1BGJ7

Security at the Edge®
Air-Gap Network Switches = Secure Hardware Access Control

Rogue access to private networks presents the greatest threat to private networks. Theft of classified information and trade secrets, corruption of data and unauthorized control of automated systems relentlessly challenge security officers and network administrators. Security patches to operating systems and software applications are updated constantly to address the onslaught of hacking that has been enabled by the proliferation of the Internet and the explosive growth of IP-connected infrastructure.

A basic but remarkable consequence of the ever-increasing sophistication (and complexity) of software security solutions is the constant introduction of unintended flaws that present new opportunities to compromise networks while identified flaws are patched. Modern software claims to be the most secure ever designed, yet news of exploited vulnerabilities in it are announced almost continuously. Evolving software security solutions offer a paradox: their increasing complexity that attempts to protect private data has provoked expanding opportunities to rogues for breaching them. It may be argued that software security will never become permanently effective and stable.

Hardware security centers on the control of the wired and wireless connections at the edges of networks and systems that tie their elements together. These solutions are air-gap switches that open and close those connections. Whether the switches are controlled manually or automatically, their points of connection to the systems and networks they protect are managed with the absolute assurance of hardware that cannot be breached by a rogue through the communications channel that passes through the switch. Properly designed, automated switch controls reside outside of the systems and networks they manage.

Hardware security solutions are traditionally applied to the control pf physical spaces like buildings, laboratories and data centers. Card and key fob credentials are commonly used to gain access to those spaces. The same credentials can be used to control access to electronic and optical data streams when specialized hardware network switches are designed to interface with the existing access controllers used to secure physical spaces. Just are access control systems manage physical doors to buildings and rooms, the same control systems manage network switches as physical "doors" to information stores.

Classified information networks have particularly stringent security requirements that must be met by any network appliance that will be inserted into classified data streams. The significant concern is isolation among connections of different classifications that are made to a switch. Coupling of data of different classifications among their networks must be prevented and specifications have been developed for the isolation among networks that must be maintained by switches that are connected to two or more networks or systems of different security classifications.

Electronic signals produce electromagnetic fields (EMF) in and around the media that carry them. These fields surround electrical cables and are the medium of communication in wireless connections. They can be detected through coupling into other conductors and by wireless receivers. Effective prevention of EMF coupling among closely-spaced electronic data cables is a substantial challenge that demands the application of unique shielding materials and techniques. Isolation of fiber optic data connections includes the same concerns when traditional methods of converting optical data (photons) to an electronic format for switching (electrons) for switching are used. Although the data is reconverted to an optical format after being switched, the intermediate, electronic stage produces the same EMF of concern in electronic network switches. Wireless data streams can presently be controlled only by enabling them or completely preventing them. There is no technology available for switching wireless data connections with the absolute security of hardware switches.

The evolution of broadband networks is driving those who demand the highest bandwidth and greatest security toward the use of fiber optic connections. Rules that govern the use of A/B network switches prevent the use of traditional switching techniques where a common connection is switched between two connections of different security classifications. Figure 1 describes this type of connection. The only solution available today employs unique micro-mirror movements to enable all-optical switching of data streams. Elimination of the intermediate electronic formats of common fiber optic A/B switches avoids the monitoring and sabotage enabled by EMF in other switches.

Software is universally used to protect private and classified information but has been found to have exploitable vulnerabilities that require constant updates and patches. Air-gap network switches provide the absolute protection of hardware to the problem of securing networks and systems against unauthorized intrusion and sabotage.
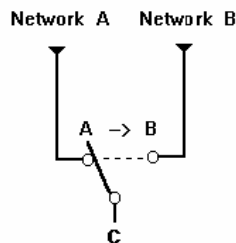

Figure 1: A/B Switch
A common connection is switched between two others
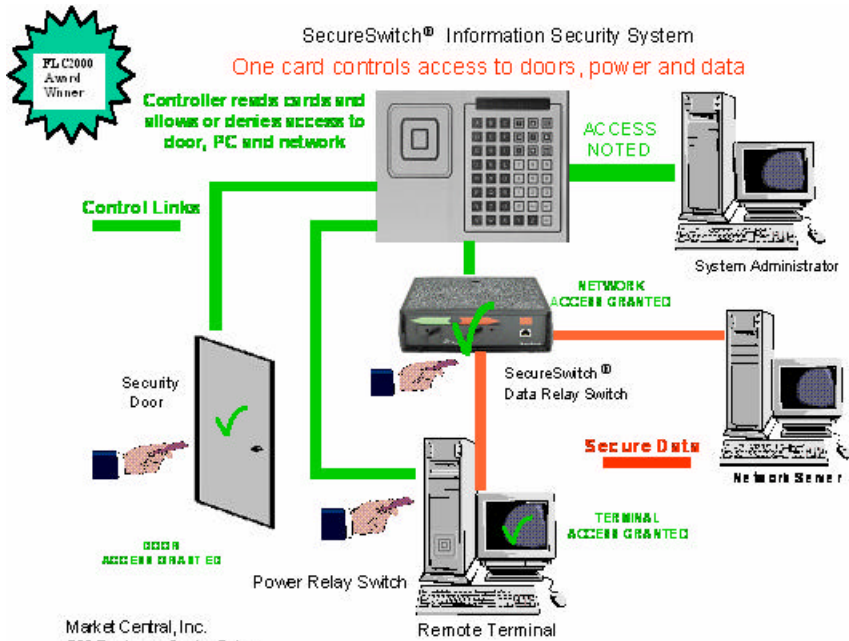
About Market Central

Development of the original SecureSwitch® Model 5000600 Dual Network Switch commenced in December of 1994 in response to a request from a U.S. Navy security officer. He had conceived the solution to a common problem of one workstation being switched between unclassified and classified information networks. The officer had purchased Market Central's commercial network A/B switches and suggested the development of a custom switch that could be produced at a low cost in quantity. The first production switch was delivered early in 1995 and was certified for use in Top Secret Naval networks. SwitchSwitch Model 5000600 was certified at EAL4 under the Common Criteria on October 2001 and was the first network switch to achieve this award. It is available at special pricing to qualified users under GSA GS-35F-0912R.

Market Central was invited to participate in a Cooperative Research and Development Agreement (CRADA) with the United States Navy in 1997. The research conducted under the CRADA yielded the SecureSwitch Information Security System. The system is protected by six U.S. Patents and includes technology from the original Model 5000600 SecureSwitch Dual Network Switch. Market Central was awarded the Federal Laboratory Consortium's FLC2000 Award for Excellence for developing this system for commercial production. The system applies existing access controllers to workstation and network management, monitoring and control and extends their features to monitor and control PC and network access; PCs and networks are literally controlled as doors to information. The system includes tamper protection and alarms.

SecureSwitch® Fiber Optic A/B/C Switch is a true A/B/C switch that controls connections of one workstation to three optical networks of different security classifications. It was certified at EAL4+ under the Common Criteria in February 2005. This switch provides 75dB of optical isolation among all connections and employs a specially manufactured assembly using micro-mirror technology that is unique to Market Central. All data passing through the switch remains in its original optical format and all intermediate electronic conversions in the data path have been eliminated. SecureSwitch® Fiber Optic A/B/C Switch is available at special pricing to qualified users under GSA GS-35F-0912R.

Summary

Market Central's SecureSwitch® network switches and switching systems are used to maintain the security of private and classified information networks where workstations connect to multiple networks of different security classifications. They are certified for that purpose and offer a hardware based solution for network security and access control applications. SecureSwitch network switches stop intruders and impose **Security at the Edge®** of the networks into which they are installed.