Homeland Security Alert.

Published: 13 September 2013

SECURE SWITCHES PREVENT DATA LEAKAGE

Protection systems for critical IT infrastructure rely on hardware as well as software. This is the case for the Advanced Secure KM (Keyboard/Mouse) Switch, Advanced 8 and 16-port Secure DVI-I KVM (Keyboard/Video/Mouse) Switches, and Display Port KVM Switch recently introduced by Belkin Business, a division of Belkin International based in Playa Vista, California. Belkin designed these products to safely isolate networks and connected systems for government agencies as well as financial institutions.

Belkin Business has specialized in designing solutions for IT infrastructure, government, academic, office and mobile environments for over three decades. The California-headquartered company has representatives in more than 25 different nations. For many years the company developed KVM switches for the data center and desktop spaces, and about six years ago, saw an important need in the government sector for desktop switching that would not allow information to cross from one computer to another.

"Our new KVM switches ensure that the information on government computer networks flow as intended and do not cross from one network to another," said Luis Artiz, director of product development at Belkin. Artiz added that one of the least understood and most under-utilized preventative measures for thwarting attacks is the use of switching devices that allow government and civilian employees to switch between networks with various security levels from one desktop location. Firewall protection alone is not enough to deter sophisticated cyber threats, noted the executive.

The Belkin executive explained that conventional KVM switches handle a lot of information through a single processor, creating the possibility of information cross-talk. The hardest part for the Belkin engineers, who designed the company's Advanced Secure KM Switch, Advanced 8 and 16-port Secure DVI-I KVM Switches, and DisplayPort KVM Switch, was ensuring that crosstalk does not occur. The team had to alter the circuit design and separate each port from the other, implementing individual processors for each port.

"We also had to design the firmware so that it would live a long time, because limited government budgets cannot upgrade computer equipment quickly," noted Artiz. Belkin used its laboratories full of combined computers, mice, and keyboards to conduct exhaustive testing and validation of its KVM switches. Indeed, validating the switches was a key factor in the design process. “To have a security product taken seriously by the federal government, it must pass the National Information Assurance Partnership standards." NIAP is an agency created by the National Security Agency to validate and certify security products by means of Common Criteria tests conducted by the NIAP for use in protecting government critical infrastructure.

After the Belkin KVM switches passed the NIAP Common Criteria tests, the California company provided samples of their switches to major defense and intelligence agencies, who then tested them internally and provided Belkin with feedback. When each agency was satisfied with the performance of the KVM switches, they would add them to their individual procurement lists.

Belkin designed its Secure KM Switch to further simplify secure switching between isolated networks by moving the mouse cursor from one monitor to another. This enables the user to transfer the keyboard and mouse controls from one computer in their network to another seamlessly without the need to press a button. While the user executes this transfer, all the other networked computers are active so that the activity on those networks can be actively monitored.

Belkin built its proven Advanced Secure data protection into the KM Switch, which also provides the benefits of a trader switch. Further, the KM Switch is equipped with uni-directional optical diodes, dedicated processors, and non-reprogrammable custom firmware to isolate the data path, prevent unintended data leakage between computers, and to prevent tampering with the switch's logic, respectively.

Each peripheral port of the Secure KM Switch has a single, unbuffered, dedicated processor to permit data analysts to work simultaneously on multiple networks at different security levels. Belkin engineers made this switch compatible with Windows, Mac OS X, and Linux platforms with USB support. The switch will soon be validated to Common Criteria EAL4+. The Belkin Secure KM Switch offers peripheral protection with USB device filtering, holographic labeling that reveals tampering, and eliminates memory buffer.

The Belkin Advanced Secure 8 and 16-port CVI-I KVM Switches are used to secure connections among peripheral devices that include audio equipment and large high-resolution displays, as well as to quickly switch among multiple personal computers and networks by means of a single keyboard, monitor, mouse, and smart-card reader. These switches, like the Secure KM, use optical diodes to establish unidirectional data paths in order to prevent leakage of information from peripheral devices into other computer systems.

Engineers designed security features into the Advanced Secure DVI-I KVM Switch family such as their protected DDC/EDID emulation to prevent software weaknesses that can cause data leakage, and at the same time, remaining compatible with the console display. The switches' uni-body chassis cuts down entry points, and the serialized holographic labels indicate tampering, thereby protecting the units from tampering.

Belkin minimizes user error by incorporating customizable color-coded ports with labels that to associate the port with the network. The switches' port button is illuminated to indicate the specific computer the console is controlling.

The growth of DisplayPort by government users in intelligence and defense has driven the development of the Belkin DisplayPort KVM Switch introduced in July, 2013. DisplayPort offers high graphics resolution with securely fastened cables, no licensing fees, and a slimmer and smaller footprint than digital video interface (DVI) cables. The DisplayPort signals are also protected in the Secure KVMs, in a similar fashion as the data and audio information.

The Belkin design team saw an opportunity in designing a Secure KVM Switch to support DisplayPort technology. The new switch is Common Criteria Information Technology Security Evaluation validated to Evaluation Assurance Level 4+, is equipped with security mechanisms that are designed to protect DisplayPort channels and prevent leakage of information between connected computers and displays. These proprietary mechanisms provide isolation even in the event of two connected computers being infected with malicious code attempting to target the KVM switch.

Artiz cited a growing trend towards securing government data on mobile devices. "More people are bringing their own device to work," he said. One way government is addressing this concern is by putting in security software like Good Technology of Sunnyvale, California. For example, the US House of Representatives and Senate use Good Technology security software on their standard Blackberry or iPhones. The challenge for critical infrastructure protection solution developers such as Belkin is monitoring the integrity of a cellular phone in a consistent manner, and furnishing that information to an IT administrator. Belkin is developing solutions to address that evolving issue.

Luis Artiz, Director of Product Management, Business Division, Belkin International, Inc., 12045 E. Waterfront Drive, Playa Vista, California 90094. Phone: 310-751-5100. Contact through: Denise Nelson, The Ventana Group. Phone: 925-837-6277. Cell: 925-858-5198. E-mail: denise.nelson@ventanapr.com.