Secure KVM switching

Assured separation with easy access

As specialists in computer switching since 1984, the engineers at Adder Technology have designed many products that transfer data between systems and this experience has been used to create the AdderView Secure range.

By returning to first principles, Adder engineers identified an exhaustive list of all real and potential vulnerabilities of standard KVM (Keyboard, Video and Mouse) switches and set about creating a new switch to counter each threat. The AdderView Secure switch allows the same keyboard, mouse and video display to be used with high and low security systems alike.

One way streets

An early problem to be identified was the danger presented by items common to both the high and low security systems that contain potentially reprogrammable elements: namely, the keyboard and mouse themselves. The threat is that either device (but particularly the keyboard) could be compromised to store information used on one network and pass it onto another network once switching has taken place.

Adder tackled this problem in an ingenious manner by taking inspiration from a common electronic component, called the *Diode*. Its job is to allow electrons to flow freely in one direction along a wire while simultaneously preventing any reverse flow. Substitute electrons with information and you get the *Data Diode*. Its sole duty is to ensure that a signal path used to transmit data from the device to the computer only ever does that, it is prevented from ever becoming a receiving line. Like much of the functionality of the AdderView Secure, the data diodes are implemented in fixed hardware rather than software to ensure that they cannot be reprogrammed and used as a tool by an attacker.

In fact, the implementation of features in solid, unchangeable electronics rather than reprogrammable software is a common theme within the AdderView Secure switch. Hardware has been used wherever possible in order to prevent subversion. Of the software that is absolutely necessary to run the internal processors, it is all contained within non-reprogrammable memory meaning that no software modifications or upgrades are possible within the AdderView Secure.

Divide and conquer

The second line of defence against a compromised keyboard or mouse takes full advantage of the sophisticated circuit separation and power control features within the AdderView Secure. Every channel is served by its own processor, signal handling circuitry and individual power supply. Whenever a channel is inactive, its links to the keyboard and mouse circuits of its respective computer are severed.

The individual power supplies for each channel ensure any potentially distinctive pulses that may be induced within one channel (due to data processing activity) will remain undetectable on the power supply or signals of the other channels. Separate memories are used to hold the various keyboard num, caps and scroll states and are only accessible once the relevant channel is selected. All data buffers are cleared once they have been used. Similarly at every channel change, the keyboard and mouse are powered down and completely re-initialised. This ensures that should any subversive reprogramming attempts manage to slip past the other defences; they will evaporate as soon as the power is reset.

Every video monitor contains a potential leakage threat in the form of its EDID configuration memory (for details, please see the Adder white paper: DDC and EDID - How video displays learned to talk back) that is used to inform computers of its capabilities. Such memory could be subverted to help transfer data from one system to another. Once again, the separated circuits for each channel within the AdderView Secure provide the safest solution: During the initial power on, the AdderView Secure harvests EDID information only once from the video display. This information is then transferred to special memories within each channel using a revolving door technique; ensuring that each computer has no way of writing data back into the shared portions of the switch.

Keep it simple

AdderView Secure employs a simple solution to prevent any external attempt at switching control subversion: The only possible method to select a new channel is to press its clearly marked front panel button; all keyboard and mouse shortcuts are banished.

Adjacent to each channel button is an indicator that illuminates when the channel is selected. Each channel is assigned a different indicator colour to assist with differentiation and to hint towards the rising importance of each connection. Thus, the indicators graduate in colour from green through blue, then amber and finally to red for the most sensitive connection (two channel models feature solely green and red indicators). The manner of switching control and indication is also intended, through simplicity of design, to promote quick user understanding and help to minimise accidental mis-connections.

Eradicating emissions

It is a fundamental law of physics that electromagnetic signals created in one device can induce similar signals in other nearby devices. This makes it possible to use sensitive radio reception equipment to eavesdrop on nearby unprotected computers. Fortunately there is a solution: Shielding. The AdderView Secure features an all-encompassing earthed steel case with overlapping panels and contacts along every edge. Additionally, there are no open access holes in the casing, which deliver two benefits: Further protection against any signal loss and also the prevention of any implements being used to probe the internal circuitry.

The battle against emissions is not limited to the exterior of the unit. When dealing

with high frequency waveforms, it is common for signals in one section of circuitry to induce a similar reaction in other sections – this is called *Crosstalk* and is particularly problematic in audio circuits. For this reason microphone connections are banished from the AdderView Secure. Also, the separated channel circuits, individual power control regions and internal shielding all cooperate to achieve at least 80dB of crosstalk isolation in the AVSC and AVSV models. 80dB means that the effect of any signal is reduced by a factor of ten thousand in each circuit, dramatically reducing the possibility of the data signals leaking from one computer to another.

Ultimate protection

For the highest security installations, each AdderView Secure model is also available in an enhanced version that adds the ability to support a security card reader while also offering two ingenious protection schemes.

The first scheme provides an opportunity for you to check the authenticity of each AdderView Secure unit. To do this, you quote the special codes printed on the unit to Adder Technology, upon which an Authentication Certificate is issued. The certificate contains a unique query code which when entered into the unit elicits particular responses (using special front panel indicators) to numeric keypresses. If the responses match those listed on the certificate then the unit is genuine.

The second special protection scheme consists of an anti-subversion monitor that continually checks for unexpected occurrences, such as dismantling of the casing, tampering with the circuitry and corruption of the authentication security information. Every five seconds an additional group of front panel indicators will perform a flash sequence to confirm that operation is normal. If any threat is discovered, the unit will permanently lock out all channels and will display a warning indication sequence.

Independently verified

All AdderView Secure units have been assessed under the Common Criteria Evaluation scheme in order to provide independent assurance that they have been methodically designed, securely manufactured and tested as fit for purpose. As a result, all AdderView Secure units carry an EAL4+ (Evaluation Assurance Level 4+) classification; giving peace of mind to security specifiers and users alike. You will find the AdderView Secure listed within the list of EAL certified products on the CESG (Communications-Electronics Security Department) website.

Additionally, the AVSV1104 model of the AdderView Secure has been Tempest tested and found to comply with Tempest level 1 requirements (USA NSTISSAM Level I and NATO SDIP-27 Level A). The other AVSC and AVSV models are sub populated versions of the same device and may be predicted to perform to the same high level.

Combined with specially designed high quality shielded cabling and approved low emission peripherals, the AdderView Secure units will provide potential eavesdroppers with an undecipherable signal level.

Creating effective protection against intrusion and eavesdropping requires a holistic approach at every level to ensure overall resilience. While the AdderView Secure does not provide the complete answer to building a secure system, it does form a significant element and it does solve the problem of how to easily access differing systems that must never be directly connected. To paraphrase Mr Gasser, the AdderView Secure has filled more than a few holes.

A summary of threats and solutions

In the table below you will find a selection of the defined threats and the counter measures developed to neutralise those threats:

Threats	Solutions
Microprocessor malfunction or unanticipated software bugs causing data to flow between ports.	Unidirectional data flow is enforced by hardware “data diodes” so data isolation doesn’t rely on software integrity.
Subversive snooping by means of detecting electro-magnetic radiation emitted from the equipment.	Carefully shielded metal case with dual shielding in critical areas.
Detection of signals on one computer by monitoring for crosstalk (leakage) signals on another computer.	No connection to sensitive analogue inputs (such as computer microphone ports) are provided. A very high level of crosstalk separation is provided between signals from different computers.
Malicious modification of microprocessor software causing data to leak between ports.	Data isolation is assured by hardware and so is not compromised by any changes to the micro-processor software. Microprocessors use one time programmable memory so flash upgrades are not possible. Case uses counter-sunk screws which can be protected by tamper-evident seals.
Buffered data within a key-board or mouse is sent to the wrong computer after switchover.	Keyboard and mouse are powered down and reset between each switchover to ensure that all buffers are cleared out.
Data leakage by means of monitoring conducted emissions on mains power.	The power circuitry provides strong protection against signal leakage via the power cable.
Data being sent to ports by means of faulty or subverted keyboards or mice causing the channel to switch and sending data in turn to each port.	Channel switching is controlled by the front panel buttons only with all keyboard hotkey or mouse switching capabilities removed from the design.

Data transfer by means of common storage.	USB ports support keyboard and mouse (and optional card reader) connections only. The product does not enable a USB memory stick or disk drive to be shared between computers. Unidirectional keyboard and mouse data signal-ling protects against data transfer across the switch.
Timing analysis attacks.	If a connection exists between a computer and a shared microprocessor system, it is potentially possible to determine what may be happening on the micro by timing the responses to repeated requests that the micro must service. For example, if a high data bit takes longer to transmit through the system than a low bit it may be possible to detect the pattern of data flowing between other ports by attempting to time the responses to otherwise normal requests. In the AdderView Secure, each port has a dedicated processor that only has input signals from the rest of the system. These input signals are only active when the port is selected. Consequently a timing analysis attack from one computer would yield no information about data flowing to another computer.
The user selects the wrong port.	Only one simple method of selecting computers is provided. The selected port is clearly and unambiguously indicated on the front panel by means of colored lights adjacent to each key switch. For high levels of security, the screens of high and low security computers should be arranged to look visibly different in general ap-pearance.
Signaling by means of shorting the power supply or loading the power supply.	Each port is independently powered by its USB port. Shorting the power supply on one port will not cause the power on other ports to be switched off.
Tampering with the switch.	The switch is fitted with tamper protection measures.
Data transfer by means of a shared smartcard.	The switch provides a layer of isolation between the physical smartcard reader and the computer. This will counter threats associated with sharing the same physical card reader. The result is to deliver the same security level as would be pre-sent if multiple card readers were used and the card was swapped between them. A further level

	of security is provided by making the smartcard function absent from certain computers (by means of using cables that lack the yellow smartcard USB connector).
Non-authentic facsimile switches.	The enhanced models enable the authenticity of the switch to be checked by means of security certificates.
Forced malfunctions due to overloaded signaling.	It is potentially possible to create forced mal-functions by constantly and quickly sending a stream of valid requests (such as the request to update the keyboard lights). A well known example of an undesirable KVM malfunction is a “crazy mouse” which was quite common with early KVM switches and was caused by data loss on PS/2 systems with the result that the mouse darted around the screen randomly clicking and opening windows. The unidirectional design of the AdderView Secure ensures that the influence of signaling on one port cannot flow past the data diodes. This means that overload signaling on one port will not affect the operation of another port. USB signalling is not susceptible to the failure mechanism that caused the crazy mouse on PS/2 systems.