Global Information Assurance Certification Paper

Created by J. Dumycz

STRENGTHS AND WEAKNESSES OF USING KVM SWITCHES OVER TCP/IP

Table of Contents

Overview

In the past, most companies' assets were tangible, perhaps a manufactured product, equipment to produce the product, and raw materials. Today, increasingly, a company's most valuable assets could be something very intangible; information. Companies rely on this information to compete in very tight markets and could be ruined if the information is lost, altered, or disclosed. This information is generally stored in electronic format. Servers can store tremendous amounts of data to be accessible in an instant, possibly from anywhere in the world. For this reason most companies have spent a lot of money to purchase firewalls and other security devices to control access to this data.

A fundamental aspect of computer security is physically securing the server and its console. If someone gains access to the console, all other security measures can be circumvented. With the advent of keyboard, video, and mouse (KVM) switches, which connect to a network via tcp/ip, access to the console of a server can be obtained from anywhere on the network, perhaps even anywhere in the world. Has this created a new security risk or can this actually improve the security posture of the organization?

This paper will attempt to examine the threats and risks involved with this remote access and the security measures that can be used to address them. It will discuss the situation before the advent of KVM using TCP/IP, and the benefits of using this new technology, along with the inherent risks involved. Five different models of switches will be briefly described. Methods of authentication, encryption, and logging used will also be discussed. The paper will then try to determine what attacks might be used and how to defend against them. Some conclusions and recommendations will then be discussed.

The focus of this paper will be on the Avocent Autoview and DS series KVM switches but models from Raritan Computer Corporation, Rose Electronics, Digital V6 Inc, and CCC Network Systems, Inc. will also be discussed.

Security before KVM using TCP/IP

For many years now servers have been protected using physical security. This was because the only way to access the server console was by entering the room and sitting down in front of it. If physical access to the console was achieved, the confidentiality, availability, and integrity of the server data could be easily compromised.

Computer room doors are almost always locked, sometimes using electronic card access systems that record anyone that enters the room, and sometimes when they leave the room. Mantraps can be used to ensure that no one enters the room with an authorized person. Walls can be hardened, in some cases using slab-to-slab construction or hardened with steel. Windows are protected or not allowed at all. The room may be alarmed and CCTV cameras

may be used to monitor access. The servers can be locked into racks or cages. Access to the room can be strictly controlled. Only personnel who have been previously authorized would be allowed to enter. This list of people could be kept to a minimum and background checks on those that are allowed to enter can be performed to ensure maximum security. Auditing of all those who enter the room can be done if the data is critical or sensitive. Once inside the room, it can be very difficult to limit the person to one or a few of the many servers inside.

Before the use of KVM using TCP/IP, all administrators who require access to any of the servers in a computer room must be allowed access to the computer room. The traffic coming in and out of a busy server room can cause safety issues for the employees. There can be a lot of wiring that could be tripped over and fire hazards caused by the amount of electrical equipment in the room. Some fire extinguishing systems can be very hazardous to humans. Reducing traffic into the server room can increase employee safety.

Benefits of KVM using TCP/IP

Analogue KVM switches were first introduced to save on the number of monitors and keyboards required. Using a KVM switch saves valuable space in the computer room by reducing the number of bulky monitors, keyboards, and mice. Using KVM using TCP/IP may also reduce the number of cables required because most models use Cat5 cable and thus reduce the wiring clutter in a server room.

With the introduction of KVM using TCP/IP administrators gain the ability to access the console of a server from anywhere on the network, potentially anywhere in the world. This access is not just access to the files on the server or to be able to run programs on the server but rather access to the server just as if he or she is sitting at the console. Access to the server is at the BIOS level. The administrator can boot the server, interrupt the boot process, and monitor it. No additional software is required on the servers.

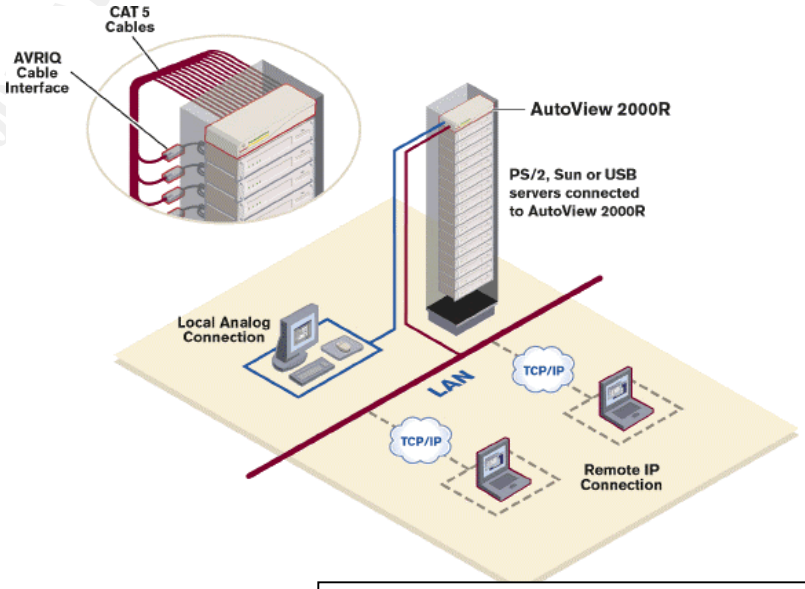

Figure 1 – (Avocent AutoView 2000R).

Being able to access all of the servers that an administrator has to manage from one place, no matter how far away they are, makes the job much more manageable. When an administrator can easily check on things and perform routine tasks from where ever he or she is, they are much more likely to be done. When the administrator is not as busy, fewer mistakes

will be made. This can lead to an increase in availability of the server, and less down time as problems are fixed faster - hopefully before they cause more serious issues.

Since security is often given the lowest priority, this can mean that more time is spent addressing security policy issues, patching systems for vulnerabilities, examining log files, and establishing procedures to ensure that data is kept secured.

Traffic in the server room can be drastically reduced leading to increased safety for employees and less accidental damage to the servers.

Companies can save money on travel for their administrators, space and shelving in the computer room. KVM using TCP/IP also offers server health monitoring. Problems can be fixed sooner, reducing costly downtime of servers. These savings can lead to the purchase of additional security software and allows the administrators more time to monitor logs and activity.

KVM Switches Available

There are many makes and models of TCP/IP enabled KVM switches available on the market today. Some of the most common are made by Avocent Corporation, Raritan Computer Corporation, Rose Electronics, Digital V6 Inc, and CCC Network Systems, Inc. They all have similar features and allow access to the server from anywhere on the network. Here is a brief description of a few of the models.

From Avocent there are the Autoview and the DS series. The newer Autoview products support up to 16 servers allowing one local user connected to the analog port, and one or two remote users depending on the model to access the connected servers. The servers connect to the Autoview switch via a unique cable called the AVRIQ. The AVRIQ contains a microprocessor and works with the switch to provide connectivity to the server being controlled. The Autoview switch also comes with the AVWorks management utility that provides auto-discovery and wizard based installation. The switch also comes with On-Screen Configuration And Reporting (OSCAR) for administration at the rack.

Figure 2 - (Nance, Feature p. 1).

The DS Series is composed of the DS1800, the DSR suite of products, like the DSR1010, DSR2161, DSR4010, and the DSR800. The CPS and SPC devices work along with the DS series. The CPS is a component that with the help of management software, allows serial devices to be controlled. The SPS, working with the CPS, provides secure power control for managed devices. Devices can be rebooted, power status can be monitored, and on/off commands can be entered. The DS1800 was the first digital KVM switch that connected via TCP/IP. DS management software includes DSAuth, DSAdmin, DSView, and DSWebview. DSAdmin software allows for information regarding topology,

permissions, and device contacts to be entered. DSAuth stores the information and performs the authenticaton when access is requested by a user via either the DSView client or the web-based DSWebview. The servers are attached to the switch using the DSRIQ smart cable and use OSCAR like the Autoview model. The SPC is a power management device that, used with the CPS (device to control serial devices), will allow for reboots of the controlled servers and monitoring of the power status.

The on board operating system for the Autoview KVM switch is Hardhat Linux. Hardhat Linux is developed and shipped by MontaVista Software. It is a pure Linux product for embedded devices. It is distributed as an opensource toolkit. In this implementation, ports 8192, 3211, 2068, and 161 are the only ports opened.

Raritran offers the Paragon, the Z-series, Masterconsole, CompuSwitch, & SwitchMan. The Paragon is composed of three main parts: the matrix switching unit, the user station (where a physical keyboard, monitor, and mouse are connected), and a computer interface module for each server. This platform can support anywhere from two to sixty-four users. Sixteen to ten thousand servers can be controlled. IP-Reach is required for access via a web browser. Using this switch allows for three different modes of access: private (exclusive access to a server), public-view (more than one user can see the server screen), and PC-share (multiple users have full access to the server).

Figure 2 – (Nance, Feature p.1).

The Rose Ultramatrix combined with the Ultralink allows servers to be controlled via proprietary windows based client software. The UltraMatrix X series connects to 4, 8, or 16 computers using special cable for lengths up to 100 feet. Multiple units can be combined using a bus connection to scale up to controlling 1000 computers. These models have an integrated auto-switching power supply.

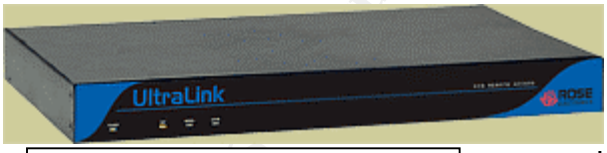

Figure 3 – (Nance, Feature p.2).

The Kaveman from Digital V6 Inc. provides TCP/IP connectivity to up to sixteen servers. Up to six users can access these servers independently. Server access is accomplished using a standard browser and Java Runtime Environment or by using VNC. The Kaveman comes in single, eight, or 16 channel models. The serial ports on the Kaveman 16 can be used to telnet to other computers if connected to a Unix machine. If one of the serial ports is connected to a smart power device, then the remote user would be able to cycle power. The serial ports can also be used in watchdog mode. In this mode and with the right server software, failed hardware or software can be reset.

Optionally, the serial port can be used to search for strings in the log files that could indicate trouble. The operating system, which is a specialized Real Time Operating System, and application software along with http, https, and VNC server software are all embedded in the hardware. This prevents viruses from overwriting the code. The firmware is flash upgradeable via the web browser.

Figure 4 – (Nance, Feature p.2).

The solution from CCC Network Systems is comprised of mini-transmitter devices connected to servers. These transmitters are then connected to a FreeVisionIP Switch. This switch is then connected to a server that compresses the information from the servers and links it to the IP network. The latest release of the FreeVisionIP Remote Network Device Management System is Version 4.0. It supports 4 concurrent IP users.

Figure 5 – (Nance, Feature p.2).

Authentication and Encryption Methods

The Avocent switches use a granular authorization scheme. This means that an administrator can decide which system administrators can have access to which servers. Unlike the scenario where access to the servers was controlled by locks on the computer room door, where once access was granted, there was no control over which servers were touched, with the use of this switch, access can be controlled. The Autoview models use a userid/password database stored in the firmware of the switch while the DS models use an organizations NT domain controller to control permissions. All data transfers are encrypted using DES and 3DES 128 bit industry standard SSL. For added security the encryption keys expire at the end of each KVM session.

The Paragon allows an administrator to set up users or groups of users with different levels of permissions. Access to individual servers or groups of servers can then be granted to these users or groups. Data transfers are protected using 128 bit SSL connections.

The Rose UltraMatrix with UltraLink uses a configuration password (which can be disabled by adding a jumper) and can use userid/password authentication for access to the switch. It does not appear to be granular enough to allow some

users access to some servers but not to others (access to the switch seems to grant access to all servers attached to it). There is no mention of encryption on their web page.

For added security the DS series from Avocent, the FreeVisionIP, and the Kaveman can use digital certificates for authentication and encryption. The FreeVisionIP solution can also use NT Domain authentication and SSL encryption and an advanced compression algorithm to increase security. The Kaveman does not use NT domain authentication. The Kaveman utilizes 128 bit SSL v2 while transferring mouse and keyboard data. All web traffic is encrypted SSL and all connections can be made using the standard https protocol. RC4 and DES are both supported. Session keys and seed values are created using true hardware random number generation. Thirty-two unique user ids with passwords can be created. The switch can operate in either "easy mode" or "certificate mode". In easy mode, passwords can be simple or disabled altogether. This could be adequate if the switch is deployed on a private network, behind a firewall and the data on the server is not overly sensitive. All data traveling on the network is still encrypted in this mode. The second mode insists on the use of digital certificates for an added layer of security.

Logging

If unauthorized access to a server console is obtained, much damage can be done. The data can be destroyed, BIOS can be changed, and of course the server could be shut down. Without the use of KVM using TCP/IP, an intruder would need to gain physical access to the server. This access can be controlled and monitored using the various methods mentioned above. Access to the room can be logged using key card access, but this does not necessarily record what servers were accessed or what actions the person entering the room performed. Normally, when the person leaves is also not recorded. With some switches an audit log can be kept of who accessed which servers, and when the user disconnected from the server. The FreeVisionIP from CCC Network Systems even offers record and play back of sessions.

In the case of the Avocent Autoview KVM switch, logging is done via SNMP via the MIB II support.

Vulnerabilities/Attacks/Defenses

Like any device on a network, these switches will be vulnerable to attacks from anywhere on the network. Some of them use browsers and java to administer the switch and access the servers. There are numerous attacks that may work on these devices. Kaveman also supports VNC and SNMP that may also be vulnerable to attacks. Some of them use NT domain authentication. There are many attacks on an NT domain controller that could be successful. The security of these switches will depend on the vigilance of the administrator of

the NT Domain servers; whether patches are applied in a timely manner, or unused ports are left open. The security profile of the server, ie if using strong passwords, limiting trust arrangements, securing all shares, renaming administrator account, using password protected screen savers, etc, will determine the security level of the switch. The switches that use their own userid/password scheme may still be vulnerable to password cracking attacks.

Both the Avocent and the Kaveman can operate in stealth mode which will help prevent attacks by being less visible to attackers. The Kaveman also has a mode called turtle mode. In this mode, the switch slows down with every failed login attempt. When enough failed login attempts are logged, the switch will send an email alert and shut down the switch. The Kaveman also does not allow any firmware to be changed by the user, therefore, the security cannot be compromised by inadvertently installing a Trojan horse or virus.

Most of these switches provide monitoring which will give the administrator earlier detection of system problems. These problems can then be immediately addressed due to the remote access capabilities.

Defense in Depth

As we have learned, security is not a product but a process. Purchasing the correct switch, or not using one, cannot provide security by itself. In order to protect sensitive data and ensure its availability and integrity, many layers of security must be applied. The first decision is whether to place the switch outside the firewall or behind it. If the switch is controlling mission critical servers or servers containing very sensitive data, then it should be protected behind the company firewall just as the servers that it controls would be. Protocols used by the switch should not be passed through any routers that they don't need to be. The more layers of security protecting sensitive, critical data, the less chance of its being compromised or destroyed. If one layer of security is broken, there will be other layers to protect the servers and their data.

If the data on the server is particularly sensitive, passwords alone are probably not good enough to protect the data from inquiring eyes. Even a strong password policy and enforcement of that policy may not protect the data. In this case, the data could be encrypted to add another layer of protection. If this is the case, it is important to implement a key management system in a very secure manner. If the keys are easily stolen, the data is not going to be very well protected. Also, if keys are not recoverable, important data could be lost by users forgetting their passwords or by leaving the company.

Another factor of defense in depth is a good backup strategy. If any damage is done to the server, either by a malicious attack or by an accidental act or by disaster, it is important to be able to recover the data quickly. If the entire building or site is destroyed, it is important to have off-site backups as well as a well-planned disaster recovery strategy. Employees must be well trained and know where to find the plan and how to begin implementing it.

Policy Issues

For any organization to secure their data, they must have and enforce a well-written security policy. Good security cannot be purchased in a piece of hardware or software. In order to manage risks, they must be identified and then communicated to the policy makers. Decisions about the value of the data must be made. Necessary measures to mitigate the risks must then be identified. Who, what, when, and why the policy is to be followed should be carefully documented. Compliance to the policy should be measurable and it should be clear who is allowed to violate the policy and under what circumstances.

In the case of the KVM switch, there needs to be an issue specific policy defined to determine who is allowed to configure the switch and which administrators would be allowed to access which servers. Also, what logging should be performed, whose responsibility it is to review them, and how long the logs should be kept would be contained in the policy. Responsibility for the maintenance of the switches should also be defined. . If the switch chosen uses an NT domain for authentication, the policy pertaining to the security of the domain controllers also controls the security for the switch.

An enterprise-wide policy could contain the rules for background checks to be performed on employees who would have access to the switch. Since either an NT domain controller or username/password in the firmware of the switch protects the switch, a strong password policy would enhance the security of the data on the servers. Also, a policy to keep operating systems patched and virus scanning software update and by whom is also important. Any policy should include any important information, be clear, concise, realistic, and easy to follow.

Deployment Methods

As with most types of devices, there are many choices as to how to deploy a KVM switch. The decision may depend on the existing Lan architecture of the organization or on the sensitivity of the data on the servers being controlled. Management's commitment to security would also influence the decision.

One of the choices would be to place the switch directly on the Internet. This may be necessary to allow for administrators to access the servers. If this is the case, it would be suggested that administrators use all available security mechanisms on the switch itself.

Another choice would be for the switch to be placed on an internal private network. This is, of course, far more secure and would be preferable in most cases. Depending on the sensitivity of the data, the nature of the authorized users of the network, and the overall security of the private Lan, all of the security features of the switch may not need to be deployed in this case.

An even more preferable solution may be to deploy the switch on a separate maintenance Lan. One benefit to this solution is bandwidth. The video data would not have to compete with other traffic on the production network. The other advantage would be an increase in physical security of the network. This maintenance network may

only have to extend from the server room to the IT department, which most likely is very close by. One more advantage is that because the network is not connected to the production network, an out of band device such as a modem, may be added to the switch. The disadvantage to this method of deployment is that Lan administrators would not be able to access the switch from anywhere else on the network.

Two other variations may be to add a firewall or filtering router in front of the switch or to deploy a VPN to access the switch. These devices may be able to offer advanced monitoring or intrusion detection capabilities.

Conclusions

With all of the constraints on companies these days, budgets are extremely tight. Any technology that can save the corporation money by reducing space requirements and technical support hours required will be of great interest to the organization. KVM over TCP/IP will provide these financial savings for many companies. But what is the cost? Does this technology create holes in the security of the corporation? Does it leave sensitive data vulnerable to attack? Or does this new technology actually improve the security of the servers being controlled by the device?

Even though these devices are vulnerable to some kinds of attacks, if the company has a strong security policy and has implemented a strong, layered defense plan, if the administrators are vigilant in their monitoring of logs etc. then the KVM switch can improve security by keeping personnel out of the computer room. Less traffic in the vicinity of the servers will reduce the risk of accidental damage to the servers or someone inadvertently unplugging a server.

In many large organizations, there are many system administrators. Often these people have responsibilities for only one or two servers in a room that may contain a very large number of servers. Once access is granted to the room, the administrator could access any of the servers. With the use of most of the KVM switches available, the administrator is limited to which server he or she accesses and even that access can be logged. Also, reducing traffic in the computer room can reduce accidental damage to servers and their connections.

In summary, these devices can improve or reduce the security of an organization. Some new vulnerabilities will be introduced but other areas of security will be improved by better access control and more logging capabilities. Since physical security is often overlooked by management, the added layer of security that a KVM switch can add is very important to the security of the data by allowing the computer room to be accessed by fewer people. Every organization needs to identify the value of their information assets to determine what level of security is required and then devise a policy and implementation plan to achieve that level of security. Good security is not purchased it is planned and developed over time. It is implemented by applying the policy in the everyday operation of the company. It is a process. With this in mind, the proper KVM device can most likely be integrated into the plan, saving the company

valuable resources and hopefully improving the security posture of the organization.

References

"Physical Security." Dedicated Servers UK. URL: http://www.dedicatedserversuk.com/security.htm (Aug 13, 2003).

"Physical Security Overview." IT Security Overview. URL: http://www2.state.hi.us/dags/icsd/ppmo/Stds_Web_Pages/IT0801/it0801s3.htm (Aug 13, 2003)

Nance, Barry. "Advancing the Art of KVM Switches." Network World. Aug 1, 2002. URL: http://www.nwfusion.com/research/2002/0819feat2.html (Aug 12, 2003)

URL: http://www.avocent.com/ (Aug 12, 2003)

"White Paper Secure KVM Access and Control" Avocent (Aug 12, 2003)

URL: http://www.avocent.com/web/en.nsf (Aug 12, 2003)

“Avocent’s KVM OVER IP™ Switching System Chosen for Microsoft® Technology Center in Tokyo”
URL: http://www.avocent.com/web/en.nsf/Content/08052003 (Aug 12, 2003)

“AutoView 2000R” URL:
http://www.avocent.com/web/en.nsf/Content/AutoView+2000R (Aug 12, 2003)

URL: http://www.raritan.com/ (Aug 13, 2003)

URL: http://www.rose.com/ (Aug 13, 2003)

URL: http://www.digitalv6.com/ (Aug 12, 2003)

URL: http://www.cccnetsys.com/ (Aug 13, 2003)

"What is KVM Over IP?" URL:
http://www.kvms.com/kvm_over_ip/what_is_kvm_over_ip.asp (Aug 13, 2003)

"FreeVisionIP." URL:
http://www.cccnetsys.com/quick_links.asp?link=%2Fproducts%2Ffree_vision_ip.asp (Aug 13, 2003)

"Rose Electronics UltraMatrix 6X." URL:
http://www.rose.com/pdf/umx-16xtechnicaloverview121700.pdf (Aug 12, 2003)

“Rose Electronics Product Overview” URL:
http://www.rose.com/pdf/ultramatrixproductoverview.pdf(Oct. 2, 2003)

"Paragon." URL:
http://www.raritan.com/public/catalog/product_line.aspx?plid=14&nav=top
(Aug 12, 2003)

Gray, Peter D. December 10, 2001. "Security Considerations When Using Kaveman"
URL: http://www.digitalv6.com/whitepapers/Kaveman_Security.pdf(Oct. 2, 2003)