Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing out-of-band device management

In networks with critical core components, securing device access while maintaining the ability to provide emergency maintenance is crucial. Often a console port, craft port, dedicated Ethernet management port or other out-ofband access must be used to recover failed devices or systems. For large networks, these devices are frequently located at remote or inaccessible locations. However, leaving the management ports attached directly or via modem presents a security hole. The network infrastructure may be very secure w...

Copyright SANS Institute
Author Retains Full Rights

AD

GIAC Security Essentials Certification (GSEC)
Practical Version 1.4
Marc S. Kolaks

Securing out-of-band device management

Abstract:

In networks with critical core components, securing device access while maintaining the ability to provide emergency maintenance is crucial. Often, a console port, craft port, dedicated Ethernet management port or other out-of-band access must be used to recover failed devices or systems. For large networks, these devices are frequently located at remote or inaccessible locations. However, leaving the management ports attached directly or via modem presents a security hole. The network infrastructure may be very secure with firewalls, IDS, and encryption systems while core access to the device's management ports is often neglected.

This paper will outline vulnerabilities of out-of-band managed systems and devices, provide worksheets for helping to ensure security and give examples of possible architectures for secure remote access.

Background:

Many network devices are managed in-band using traditional applications and protocols. Internal web servers, SNMP access, Telnet, Secure Shell and proprietary interfaces provide the day-to-day configuration and auditing. These layers are typically protected by security including access control lists, Userid / PW access from cleartext through encrypted secure tunnels, and/or disabling certain management services.

However, most devices have out-of-band access ports that provide access to the core configuration in the event of a catastrophic failure of the normal in-band management methods. These ports come in many varieties including TTY serial ports, direct console access (keyboard, video and mouse) and dedicated Ethernet IP management ports. Some devices, including various ISDN terminal adapters, have analog telco interfaces providing a method of resetting configurations using DTMF signaling from a touch-tone phone.

[*Note: Since it fits into the architecture described in this paper, and since normal console access of a network device or server is not typically the way that the production access occurs, direct console access, that is, Keyboard, Video and Mouse, of network devices will be considered out-of-band access*.]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Company security policies, generally, will restrict or prohibit a dedicated connection to these ports through modems or other access methods. In practice, however, the requirements of system availability often lead to unsecured access points. Those responsible for keeping the devices and networks running will leave a back-door access in place on these ports so that disastrous failures can be rapidly fixed.

To address these vulnerabilities, organizations should provide:

1) Definitions for vulnerabilities and risks of out-of-band access.
2) Security Architecture for mitigating those risks.
3) Proper balance between security and the need for timely out-of-band access during critical events.
4) Systems of processes, equipment and technologies that provide, where required, integrity, confidentiality and/or non-repudiation for out-of-band access.
5) Mechanisms and/or processes for auditing out-of-band management.

By offering a security framework that provides for out-of-band management access, security of the entire enterprise architecture is enhanced.

Definitions for vulnerabilities and risks of out-of-band access.

When developing Information Security policies, plans and architectures, do not ignore the vulnerabilities of *all perimeters* including management access ports. Two major incidents documented by NIST, the National Institute of Standards and Technology, occurred because of unsecured maintenance ports. At Time Warner Cable, intruders were able to gain access to systems that controlled satellite broadcasting and positioning, "The intrusion itself was reportedly perpetrated by dialing directly into Time Warner Cable's system through a maintenance port."[1] A juvenile hacker disrupted phone service to an airport control tower and an entire town in Massachusets through a maintenance port in a NYNEX Telco office, "The local loop systems attacked by the hacker had been left accessible to public phone lines by Nynex phone company employees, who occasionally repaired the systems remotely."[2]

For every network attached device having out-of-band management access, document the vulnerabilities of that access and the risks if that access is compromised. An appropriate way to accomplish this is to either ensure that this is incorporated in preexisting documentation or develop a separate worksheet for management access port security. Be sure to include not only the technical specifications of the type of access (for example: serial, management console, network) but also the control that the management interface provides (for example: system shutdown, default configuration restoral, non-authenticated access).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Another risk to define is the consequence to system availability and stability if the out-of-band access is not readily available. Detailing this risk will help in balancing protection with the need for timely maintenance of crippled or disabled devices.

An example worksheet is provided at the end of this document as a template for developing your own.

Security Architecture

With any system, device or function in Information Technology Security, proper design of a security architecture is the foundation of protection. For these critical devices and systems, protection is of the highest obligation.

A security architecture must address confidentiality, integrity, non-repudiation, availability and auditing / monitoring. The management or maintenance access of the devices and systems described in this document, should, like any component of an IT infrastructure, be supported and guided by this architecture and its contributing processes. This paper does not cover the details of creating a security architecture. There are many resources for defining a security architecture and developing security policies, standards and guidelines. For further information, see the resources listed at the end of this document.

For the purposes of this document, a brief overview of elements of a security architecture along with relative examples, is helpful.

> *Confidentiality*: The protection against access of private or personal information as well as defining the duration that the information must remain private. Examples include the management access userids and passwords, an access control list on a router, and phone numbers of dial backup systems of Wide Area Network connectivity devices.
>
> *Integrity*: The protection against improper alteration or modification. Examples include preventing modification of management userid information except by specific user roles, preventing human modification of routing information (machine-to-machine route table updates only), and procedures for backing up device configuration to off-line storage.
>
> *Non-repudiation*: Preventing denial of actions or events and providing proof of delivery and reception of information. An example of a repudiation of an event could be – An unprepared engineer mistakenly clears dynamic configuration information on a device, preventing access to critical resources for all users. Realizing his mistake and knowing that it takes 2 hours for the tables to be rebuilt, he logs out of the systems and denies any interaction with the device.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Availability: The resilient and timely access to systems and information. Examples include requiring down-time to be scheduled at least 14 days in advance, ensuring that security controls do not hinder the timely access to information, and providing redundancy for critical systems.

Auditing / Monitoring: Providing a process for both real-time monitoring of events and post-event examination. Examples include sending a SYSLOG message for all management port access and discrepancy comparison of pre and post configuration changes.

Classification:
A requirement of developing a security architecture is defining and applying a process for the classification of information. A typical delineation is public, internal, confidential and restricted. Since the details of Information Classification are out of the scope of this paper for further definitions and details, please see the resources listed at the end of this document. The main thing to keep in mind concerning Information Classification and out-of-band management port access is that very often, the classification of the information of the production systems of a device are quite different than the classification of the information accessed by the management port. For example, a public web server has a repository of information classified as public, while the configuration of that server accessed by the management interface could be considered confidential or restricted.

Out-of-Band management access security standards

Organizations may have different models for implementing a Security Architecture. Since the end-state of implementation of security infrastructures and processes is the same no matter what model is used, this paper will assume the following:

- A single Security Policy drives the Security Architecture.
- A separate Security Standard is developed, describing the general requirements for Out-of-Band management port access.
- Multiple Security Guidelines describe the technical details of the systems and processes identified in the Security Standards, up to and including product selection and configuration.

For some organizations, this hierarchy is shifted. Multiple security policies may exist, with one addressing Out-of-Band access. The standards, then, would address the technical details of the security systems and process. Guidelines, if they exist, may outline procedural details for implementation and management.

Since there are literarily thousands of different network devices with management port access, hundreds of access methods and hundreds of vendor solutions, the Security Guidelines have a high likelihood of being unique. Security Standards, however, may be very similar across organizations.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security Standards should be developed at a generic enough level that not only is the current environment addressed, but realistic future environments as well.

As a driver for creating the standards, document and organize the risks and vulnerabilities for the Out-of-Band accessed devices. Even if the configuration of the production capabilities of a device are unreachable through the management port, other vulnerabilities, such as remote power cycling, might be accessible. A table format, such as the following example, is helpful in this organization:

Vulnerability	**Risk**
Restoral of device's factory defaults	Device configuration can be lost causing complete failure
Reconfiguration of device's IP configuration	Proper routing of production data can be compromised
Production access control information can be obtained and/or modified	Unauthorized access to production systems can be obtained
Device power can be cycled	Availability of production systems can be compromised
Any access through the management port causes the device to stop all production processing	Access will cause system unavailability.

For each of these example vulnerabilities and risks, all 4 areas of security can be affected: Availability, Integrity, Non-Repudiation and Confidentiality. This helps stress the necessity of including Out-of-Band management port access in security architectures.

The following outline can be used as a template in developing a Security Standard for Out-of-Band Device Management.

1 Overview
Provide an overview of the standard's purpose. If necessary, include a background section that describes the drivers for creating this standard such vulnerabilities and necessity of timely management access. In addition, reference the overriding Security Policy statements.

2 Risks and Standards
This section will list the individual risks and the required standards to mitigate those risks. Some examples follow.

2.1 Vulnerability/Risk – Manufacturer management accounts and passwords are easily obtained through publicly available documentation, providing a risk for unauthorized access

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Standard – All default accounts will be disabled, renamed, and/or removed. All default passwords will be changed.

2.2 Vulnerability/Risk – Modems can act as a backdoor to management of devices, bypassing other network security systems. War-dialing techniques can be used to find unsecured modems.

Standard – Modems will be used to connect to management ports only when no other option is available (for example, at an inaccessible location). All modems attached to management ports must use a touch-tone password access device before a synchronization tone is presented. If possible, caller-id service and a supporting modem should be used to allow access from designated phone numbers only. If a high level of confidentiality is required, hardware encryption modems should be used at both ends of the connection. All modems not meeting these requirements must be disconnected and removed from service.

2.3 Vulnerability/Risk – Some management ports have no authentication systems in place for access.

Standard – Any management port that does not have authentication control must have an authentication system or device installed. This system can be shared between multiple devices if the access control can be managed in a granular enough method. This system must be separate and distinct from normal production authentication systems and connected directly to the device or to a management network.

3 Review and modification process. This section should describe the procedure for regular review of the standards and provide a method for modification when necessary.

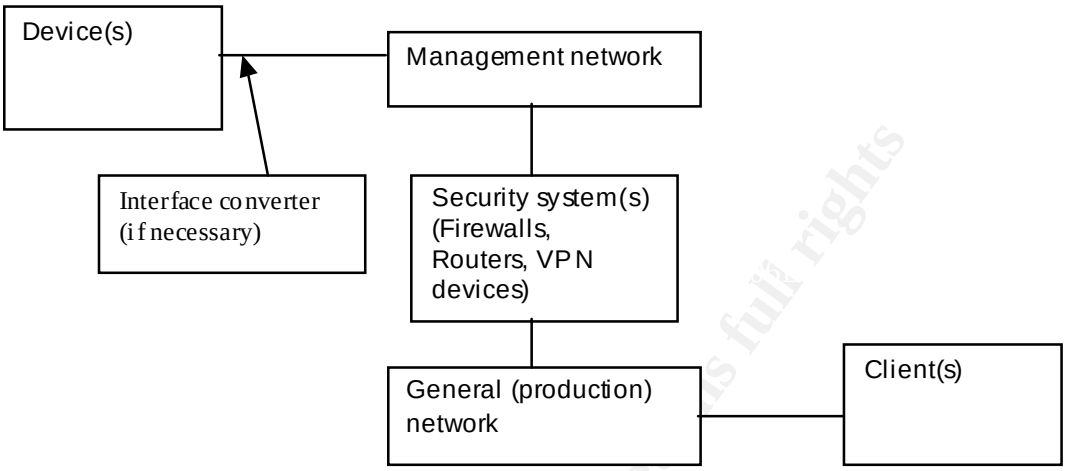
4 Glossary and Terms. This section should define unfamiliar terms and technologies referred to in the document.

Applying the standards to develop guidelines

The technical detail of the security architecture should be presented in guidelines. These guidelines should provide a level of detail generic enough to aggregate configuration procedures across different devices and systems.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A good approach to device management security is to divide the access path into logical segments or domains, providing a dedicated management network. Illustration xxx gives an example.



Using the definitions and documentation previously created, categorize the devices into logical management groups. The characterization of these groups will depend on many variables including the level of security required, the geographic placement and the management interface type.

For example, consider a network with the following components:

Device	OOB mgmt port	Location	Accessed by
RouterA	RS232	HDQ	Network Admins
RouterB	RS232	Plant1	Network Admins
Switch1	RS232	HDQ	Network Admins
Switch2	RS232	HDQ	Network Admins
Switch3	RS232	Plant1	Network Admins
Switch4	RS232	Plant2	Network Admins
IDS	Ethernet	HDQ	Security Admins
CoreSwitch1	Ethernet	HDQ	Network Admins
Firewall	KVM (Keyboard, Video, Mouse)	HDQ	Security Admins
Content Filter	KVM (Keyboard, Video, Mouse)	HDQ	Security Admins

The first attribute to categorize on is location. While Out-of-Band or dedicated management networks can be interconnected with secure routing protocols, the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

equipment directly connecting to the devices cannot be shared across locations. In this example, 3 management 'networks' are defined, HDQ, Plant1 and Plant2. Since HDQ and Plant1 have multiple devices, it may be possible to share the management network at these locations.

A management network may or may not be comparable to a traditional data network. For use in this architecture, the management network should be considered a connection method between security systems and physical device interface or interface converter. This network may be shareable among other devices, may be dedicated to a single device and/or may even be combined with the physical device interface and security system into a single piece of equipment. In some cases, the management network may be a traditional IP network.

The next attribute concerns who needs access to which devices. In this example, two roles exist, Network Admins and Security Admins. Depending on the devices' authentication systems, a simple userid / password may be sufficient to limit access. However, in this example, we will assume that the Out-of-Band management ports have no authentication method internally available.

Two different methods are available to separate access for the two roles. The most direct approach is to segregate the equipment into different management networks, each with its own security system providing access authentication. Another method is to employ a security system that has the ability to provide role-based access to allowed devices through a single interface to the entire management network.

The third, and in this example, last attribute is the physical device connection. Since there are 3 different types of device interfaces listed, ease-of-use would be increased by finding a common denominator using various interface converters. In addition, combining the access through the management network can provide economies of scale by providing a method for using single security systems across multiple devices.

For the three interfaces listed, RS232 serial, Ethernet and KVM, devices and technologies exist that allow all three to utilize IP networks. Serial interfaces can be accessed through terminal servers. Ethernet interfaces are likely to be native IP by default (and if not, protocol conversion devices are available). Devices also exist that convert KVM access to IP, giving accessibility through IP networks to proprietary applications on client machines.

Some example guidelines, supporting the standards and policy, that can be created from this information could be:

- Where feasible, all devices having the same security domain attributes (Interface, Location and Access), should share the same authentication mechanism. A VPN connection through a common gateway should be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

used for any connection of a client to any device on the management network. If a centralized authentication / authorization system such as TACACS is available, it should be used.

- Devices with console access via a standard VGA monitor, keyboard and mouse, should connect to a KVM switch that supports IP access.
- When selecting terminal server equipment for serial RS232 management port access, the equipment should support SSH authentication. In addition, multiple device access should be aggregated on multiple port terminal servers where physical limitations are not a barrier.
- Where possible, shared user accounts should not be used for device access. Instead, individual user accounts should be used. Where this is not possible, individual user authentication should occur at a security system, with final access to the device via the shared login.

Notice that each guideline contains the directive "*should*". Since Out-of-Band management access is very often unique to each device manufacturer and model, the guidelines may be generic enough to cover many different implementations. Detailed systems for connecting and accessing a particular device may be documented in separate procedure documents for each device.

Summary of Policies, Standards and Guidelines.

In the previous examples, one method of incorporating a security architecture is presented. In some organizations, the definitions and nomenclature of Policies, Standards and Guidelines may be quite different. As an example, an organization may have a separate policy encompassing Out-of-Band management access only, with individual standards documents for each type and/or version (manufacturer and model) of device. This architecture documentation may not have any guidelines created and may rely on all details being presented in the standards.

No matter what formal methods are used for developing and documenting a security architecture for Out-of-Band access, the end result should be the same: Providing an architecture that addresses Availability, Integrity, Confidentiality and Non-Repudiation. The same information must be gathered – access methods, equipment details, risks and vulnerabilities, to name a few. The same solutions provided, such as authentication and access control systems, audit/logging systems. And the same balance of availability versus security.

The next section will explain the importance of maintaining this balance in developing this architecture.

Balance

When creating and defining a Security Architecture for Out-of-Band access, the costs, both tangible and intangible, must be a factor. These costs include not

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

only the real costs of researching, procuring and implementing technologies and processes to address the architecture, but also any increased costs associated with system availability due increased complexities dictated by this architecture. Let's look at both ends of the spectrum. For a particular device, simply not connecting the management port eliminates, as long as the device is in a physically secure location, security issues associated with access through that port. The material costs to do this are zero. However, if that device is critical to production systems and recovery requires management port access, then the cost of the time it takes to connect to the management port, access the device and restore production must be considered. If the device is at a remotely inaccessible location, this time can be considerable.

On the other hand, if a device is connected to a secure terminal server, through a VPN gateway using one-time passwords and has hardware encryption devices at both the device and client ends, procurement, implementation and on-going maintenance can be very expensive. Rapid, secure access to the management port through the network is provided. If the management port access is by personnel staffing 24x7, real-time monitoring network operations center, then recovery time will not be extended because of lack of immediate availability to the management port. However, if the device has its own high-availability or redundant systems or the availability of the production systems it services is not critical, then the cost of this system is out of proportion.

When developing the architecture, make sure to include the ability to group device access and reuse technologies and systems where appropriate. A typical problem with Out-of-Band management systems is that one access role is often oblivious to similar requirements of another. If work has been done to address Out-of-Band security requirements in one area, those systems can frequently be reused in another area. Even if the security technologies and systems of existing device management access are above and beyond the requirements of a new need, the economies of reusing and/or reapplying this existing infrastructure to future systems must be considered in the balance as well.

It is very easy to get wrapped up in the latest technological 'gizmo' and spend money unnecessarily on security products. Remember, as quoted so much as to be ubiquitous in Security literature, "Security is a Process, not a product"…and part of this process is providing a balance between the mitigation costs and the exposure costs. However, because the exposure of compromised management port access can affect not only a deeper level of integrity, but a broader range of systems, the costs of safeguards and countermeasures is usually not difficult to justify.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Systems, technologies and equipment

Dedicated management network

Implementing a network dedicated to the management of network components can provide a higher level of security. Keeping the management traffic separate from production traffic allows not only better access control, but, may also provide access when the production infrastructure is down due to denial of service-type outages. Depending on the level of isolation, the management network may be unaffected by these types of outages, whether accidental or malicious.

Building a management network requires some type of logical or physical partitioning from the production network. Ideally, the management network should exist on its own physical network. Connection to this network can be controlled by having directly attached dedicated management clients, router access control lists (ACL's), firewalls and/or VPN systems.

If accessing the management network from clients attached to the production network, consider the need to prevent eaves-dropping on the management traffic. A VPN solution providing encryption will address this. If the confidentiality of the management traffic is not a concern and access will be entirely within internal networks, then a firewall or router may be sufficient for separating the management network.

[*Note: Any perimeter firewall or router, even if not part of a management network infrastructure, should be configured to prevent access to the management network from the outside. In addition, routes to the management network should not be advertised outside of perimeter routers. If access from the outside is necessary, a secure VPN solution should be implemented to provide for this access.*]

For management of network elements in a telecommunications environment, an entire spectrum of documented standards, requirements and methods are available. The International Telecommunications Union (www.itu.int) has a series of recommendation documents related to management networks. Refer to the links at the end of the paper for more information.

Serial port access

Most network infrastructure components have an RS232 serial port for direct management access. While access control to these ports is often secured by the physical location of the device, this often leads to difficulties in the ability to use this access in an easy, timely manner.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

One approach is to connect the port to a terminal server. A terminal server provides IP access through a telnet or secure-shell connection from a remote client. Typical terminal servers are available in multiport configurations. While this may be appropriate when managing multiple devices in a single location, infrastructure devices are frequently apart from other systems. In these cases, single port terminal servers are available.

Some components have the ability to use centralized access control mechanisms. For example, Cisco's TACACS Terminal Access Controller Access Control System, provides centralized validation of users accessing Cisco network equipment. Another method available from numerous equipment manufactures is to use a RADIUS authentication server. RADIUS can even be linked to existing directory or access control structures including Microsoft's Active Directory®, Novell's eDirectory® and IBM's RACF®.

Analog phone interface

In cases where the only practical management access is through a dial-up connection, special effort must be used in designing secure controls. Typically, this phone connection is via the PSTN, Public Switched Telephone Network, and, as the name states, it is accessible to the public. Unless controls are in place, dial-up modem access is often the most vulnerable point of any system. Even if the device is plugged into a phone port on a private PBX and inbound external calls are prohibited from connecting to this port, a malicious individual may gain access by requesting a transfer to a specific extension. There are various technologies and configurations to help control this vulnerable access.

Dial-back - A common option that forces the device to call back to a specifically configured number when a connection is attempted. When a management access is required, the user dials the number associated with the device. The device answers, hangs up, and then calls a pre-configured number. This should be the modem phone number of the management client. Some configurations allow for identification of a user and will dial-back a number associated with that particular ID.

Caller-id – Not as common as dial-back, this option will only accept calls from specific, pre-defined phone numbers.

TouchTone password device – This is an inline device that requires a distinct password to be entered using touch-tone numbers. It is similar in concept to entering calling card digits after dialing a phone number. The device will not present any modem tone until the proper password is entered. These types of devices can provide a barrier to war-dialing.

Secure Modem – This system requires a specific, pre-configured modem at each end of the connection. They are available in one-to-one, one-to-many and many-

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

to-many configurations. That is, a pair of modems can be dedicated to each other so that no other modem can talk to the other, one device modem may be accessible by many, pre-defined client modems, or many device modems may be accessible by many, pre-defined client modems. These devices are usually costly but often provide the added benefit of end-to-end encryption.

Token-based device – Uses a time-based, one-time-password to permit access. Some modems will have this feature built-in, providing a configuration similar to the Secure Modem described above. This allows the use of normal, off-the-shelf modems for the client side.

Many vendors offer solutions for providing a single secure modem access to multiple devices. These solutions are typically more cost-effective than deploying dedicated modems and phone lines to each device.

If secure modems or token based authentication are impractical, consider combining multiple technologies where possible. For instance, configure a device accept connections only after passing through an inline touch-tone device, from specific phone numbers (Caller ID) and dial-back to preconfigured numbers after authenticating the user. In-line password devices are susceptible to brute force attacks. Caller ID restrictions can be bypassed through call-forwarding or social engineering. Some dial-back systems are vulnerable to a malicious user mimicking a hang-up signal and then waiting for the modem to attempt the out-bound dial, providing a fake carrier, ring and answer. However, by combining multiple technologies, modem access is more secure.

Console access (Keyboard, Video and Mouse – KVM)

An often overlooked aspect of system or device management is the actual keyboards and video monitors attached to server-based platforms. Since access to these systems through KVM's is not typically for production use, KVM's can be included as part of the management infrastructure.

In the simplest form, KVM access can be controlled by physical isolation of the equipment, however, as in the previous systems, this can present a barrier to rapid access when emergency maintenance is required. Often, remote control applications (e.g. PCAnywhere, Remote Admin or VNC) are used for this access. The problem with using remote control applications is the need to gain access through a traditional network interface. Even for software that can be bound to a specific NIC, dedicated to the purpose of management, this can cause greater risk by providing a dual-homed system. If the system is ever compromised through the production interface, then the entire management network is vulnerable.

Two possible solutions are system management interface cards and IP-based KVM switches. Management cards allow an IP connection to the keyboard,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

video output and mouse. This interface provides access only to the KVM subsystem. IBM, HP and Dell all offer integrated out-of-band management cards that provide remote console capability. Companies such as Cyclades, American Megatrends (AMI) and Intel have management cards that are system vendor independent. Intel also manufactures motherboards that have remote management interfaces built-in.

IP-Based KVM switches physically connect to the keyboard, video and mouse interfaces on a system and allow access with special client software over IP. The benefits of these systems include complete independence of the hardware platform, no use of resources on the server and the ability to control multiple systems from a single KVM switch box. Avocent, Rose Electronics, Raritan and Startech all manufacture IP-based KVM solutions in addition to traditional KVM switches.

Although these switches typically have their own internal access and authentication systems, they should be connected to the dedicated management network to take advantage of additional access control features of a management network.

Auditing

Since access to management sub-systems exposes systems at the most vulnerable levels, proper auditing must be in place. Where possible, all access transactions, whether successful or not, should be logged to a separate logging facility. Many devices provide the ability to use Syslog message to track access and authentication events. Some devices, however, provide for remote logging, but only through the production interface. This means that deployment of a logging system might be required not only on the management network, but also on the production network.

Any unsuccessful access should cause an immediate alert to be generated and forwarded to a real-time (or as close to real-time as practical) monitoring system. This system can range from a console display at a 24x7 staffed operations center to email or pager notification. Audit logs should be reviewed on a regular basis.

Once a management infrastructure is in place, any new systems or devices requiring management access should go through a checklist process before attachment to production facilities. An example checklist is included below.

Conclusion

Management interfaces of critical systems provide not only necessary access to configuration and maintenance, but also present a high potential for exposure. Developing a security architecture addressing out-of-band management will help provide a balance necessary for timely, secure access.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Example checklists and worksheets.

These are included to provide a starting point for developing your own checklists. They are not inclusive of all issues and configuration variables relating to out-of-band management of network devices.

Dedicated Management Network	
Is the management network logically and physically isolated from the production network by a router?	
Do Internet connected routers have routing turned off from the Internet to the management network?	
Is the management network physically secure?	
Access control	
Is access to the management network controlled by ACL's on the router?	
Is the management network isolated by a firewall?	
Is access to the management network from the production network tunneled through a VPN connection?	
Are access logs available with processes defined for regular review?	
Are the routers, firewalls and/or VPN devices configured to send real-time alerts for access or authentication denials?	

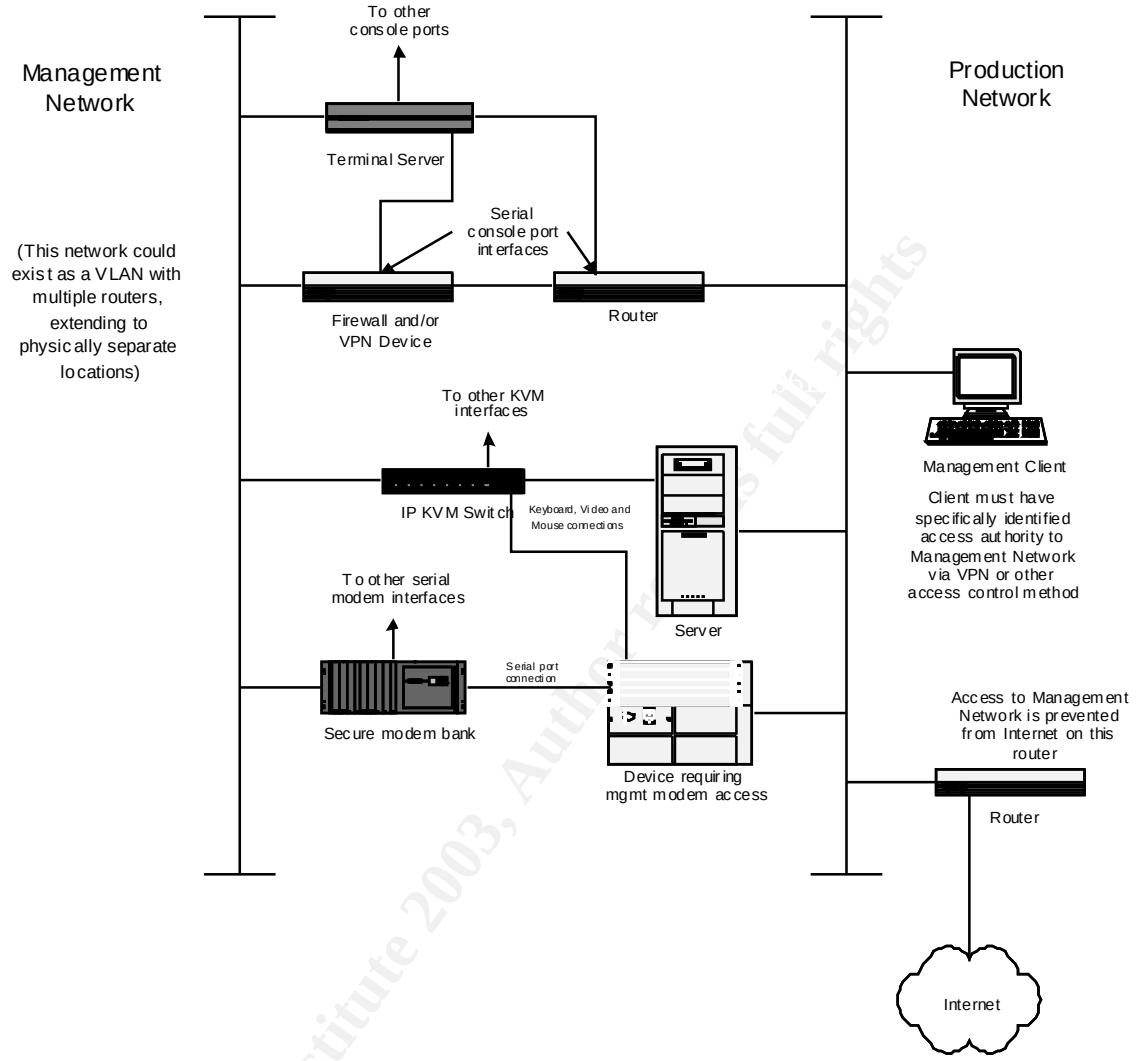
New equipment management worksheet			
Manufacturer		Model	
Device Type			
Management interface(s) (serial, Ethernet, modem, console)			
If IP based management is available, is the Ethernet port physically separate from the production interfaces?			
What IP based access methods are available (HTTP/HTTPS, SNMP, Telnet, FTP, TFTP, SSH)?			
Access control methods			
Single UserID / PW?			
Multiple UserID / PW?			
Role based authority?			
Vendor specific (e.g. TACACS)?			
Radius?			
Other?			
If management modem connection is required…			
Is caller-id authentication available?			
Is dial-back control available?			
What access and authentication logging capabilities available?			

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Managed network device checklist	
Have the default management IDs and passwords been changed?	
Have all unnecessary management access methods been turned off or disabled? (e.g. SNMP, HTTP, Telnet, etc.)	
If a management modem is required, have proper safeguards (call-back, Caller-id, secure access device) been installed and configured?	
Has a remote logging facility been configured?	
Has a known good time source been configured to ensure proper log file timestamps?	
Have access roles been defined?	
Have internal management control parameters (e.g. allowed IP addresses, time-of-day restrictions) been configured?	
Is there limited physical access to the device?	
Are inactivity timers configured for management sessions?	
If a management session is interrupted, is the system configured to prevent reconnection without logon?	
Is the system configured to disable logins after x number of unsuccessful logon attempts?	
Is the last successful logon time and date displayed upon successful logon?	
Is the system configured to send real-time alerts in the event of an unsuccessful access or authentication attempt?	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Example implementation of dedicated management network



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Equipment Links– *(The vendors and links are listed to provide a starting point for researching various products and technologies. They are not endorsed or recommended by the author.)*

Western Telematic, Secure modem solutions, Remote console access – http://www.wti.com

Computer Peripheral Systems, Secure modem and management control devices - http://www.cpscom.com/general/prodalph.htm

Ion Networks, Token based management access sytems - http://www.ion-networks.com

ServerTech, Remote Power Management - http://www.servertech.com

Datacomm for Business, Inc., Access Switch RS232 console access - http://www.dcbnet.com

GDC, Out-of-band management access solutions - http://www.gdc.com/

Avocent, KVM solutions – http://www.avocent.com

Rose Electronics, KVM solutions – http://www.roseelectronics.com

Raritan, KVM solutions – http://www.raritan.com

Startech, KVM solutions – http://www.startech.com

List of References

Borland, John. "Feds charge underage hacker" Net Insider 18 March 1998 URL: http://www.techweb.com/wire/story/TWB19980318S0022 (15 Sep 2002)

White, Gregory B., Ph.D. "A Common Weak-Link in the Security Chain" Gregory B. White, Ph.D. 1999
URL: http://csrc.nist.gov/nissc/1999/proceeding/papers/p35.pdf (15 Sep 2002)

Glitho, Roch H. and Hayes, Stephen. "Telecommunications Management Network: Vision vs. Reality" *IEEE Communications Magazine*,March 1995 URL: http://www.comsoc.org/livepubs/surveys/public/2q99issue/reprintone2q.html (15 Sep 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Kindervag, John. "First Steps in Achieving Network Security" osOpinion.com 14 May 2002 – URL: http://www.osopinion.com/perl/story/17752.html (15 Sep 2002)

Opening Technologies "Network Management Based on International Standards (OSI, X.700, and OMNI*Point*)" URL: http://www.corecom.com/ftpdir/pub/corecom/x700.pdf (13 Oct 2002)

Rauscher, Karl. "Network Reliability and Interoperability Council Best Practices" URL: http://www.bell-labs.com/user/krauscher/nric/ (13 Oct 2002)

CommWeb.Com. "Remote, Out-of-Band Network Management" 28 May 2002 URL: http://www.commweb.com/article/printableArticle?doc_id=COM20020528S0001 (13 Oct 2002)

King, Christopher M., Dalton, Curtis E. and Osmanoglu, T. Ertem Osmanoglu Security Architecture: Design Deployment and Operations Berkley: Osborne / McGraw-Hill, 2001

Footnotes

[1] http://csrc.nist.gov/nissc/1999/proceeding/papers/p35.pdf

[2] http://www.techweb.com/wire/story/TWB19980318S0022

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced