Closing the Four Security Risk Gaps of Mainframe Console Access

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for I/O Concepts

November 2008

IT Management Research, Industry Analysis, and Consulting

EMA

Table of Contents

Executive Summary

The mainframe has long been viewed as an inherently secure environment. Today, that view may be obsolete. The locked door and logical segmentation have fostered a belief in the insulation of the mainframe from the threats that plague the distributed environment. Those beliefs may be little more than myths when confronted by the reality of modern computing, where IT resources can be accessed from anywhere—from inside as well as outside the physical walls of the business.

As the gatekeeper of fundamental System z control, the mainframe system console must be a high priority in defense.

Nowhere is this more evident than in the exposure of the mainframe console. As the gatekeeper of fundamental System z control, the mainframe system console must be a high priority in defense. And yet:

- Increasingly, system console access is extended to both public and private networks. Not only does this eliminate the locked door, it exposes the console to security threats that have grown enormously in recent years, resulting in significantly decreased control over who can connect to the console itself—from internal as well as external networks.
- Nor is the locked door as airtight as many think; security measures for local console access often do not significantly reduce the risk to the enterprise. From system programmers to maintenance and housekeeping personnel, many more have access to the console than the business may want to acknowledge. Although RACF, ACF2 and Top Secret are tools of impeccable pedigree for managing access to mainframe-specific data and applications, few organizations control console access with these tools because of the problematic burden to data security staff and the negative impact (even when properly configured) to operator productivity.
- Without finely-grained access control and visibility into privileged activity, sensitive mainframe console access may be based on trust alone—a risk exploited in increasingly visible incidents where highly skilled professionals have "gone rogue" with business-critical information assets.
- Exacerbating these console access risks are the declining numbers of mainframe professionals and the preponderance of security staff lacking mainframe expertise. This knowledge shortfall leads to flawed assumptions, incomplete analysis, and faithful acceptance of assurances.
- These factors raise not only security risks, but potential business and compliance risks as well.

In this ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) paper, EMA explores the four major risk gaps of mainframe console access. The I/O Concepts ioEnterprise solution for secure local and remote console access is examined for its values in replacing obsolete assumptions of mainframe security with verifiable network security and access control. Executives as well as mainframe and security professionals will gain new insight into the risks exposed by remote mainframe console access, as well as an appreciation for a solution set that offers flexible console access with proactive control.

Introduction

If an IT professional were asked to name an inherently secure environment, chances are they would cite the mainframe. Its role as a dedicated business asset is highlighted by the historic discipline of its unique administration and use. Physical as well as logical isolation characterizes the typical mainframe deployment, with physical access intended for only a few dedicated professionals. This is not an environment for "ordinary" users—a fact which has historically kept it free from some of the most troublesome issues that plague security in distributed and desktop computing. This, however, is no longer the case.

*Today, the realities of modern computing and IT security have exploded the assumption that the mainframe is **inherently** secure.*

Today, the realities of modern computing and IT security have exploded the assumption that the mainframe is *inherently* secure. Inside and outside the enterprise, access to business-critical resources from anywhere, at any time, is more than just expected of IT; it may be *required* in order to optimize workforce flexibility and maximize the return on the personnel investment. When access to the mainframe must be more widely extended—an inevitability considering its importance as a business asset—new risks emerge that may completely bend or break legacy mainframe security models. Remote console access may be required from the home or small office/home office (SOHO), from public wireless access points, hotels, airports, partner sites, and a potentially limitless range of other possibilities. This potentially exposes the mainframe to anyone who can access a network traversed by a remote console protocol—including malicious individuals anywhere, regardless whether they are trusted insiders or external attackers.

Inside the enterprise, threats may be just as significant as outside. Even when there is no malicious intent, threats that find their way onto the desktop can plague highly skilled professionals as much as ordinary users. When insiders do pose a trust risk, many models of access control enable far too much latitude in user actions with little or no effective defense against threats—regardless whether console access is local or remote.

And yet many enterprises remain ignorant of these risks, trusting instead in a sense of mainframe security that may, in fact, have been rendered obsolete by ubiquitous network connectivity and remote access. The malicious, however, are most definitely *not* blind to these realities. Nor are regulators, who can be expected to take a much harder look at these issues in the wake of increased threats and exploits that have had both a high dollar cost as well as widespread personal impact on the millions victimized by information security breaches.

Mainframe Console Access: Four Areas of Concern

The risks of mainframe console access fall into four principal areas:

1. Consoles are generally not as secure as believed, especially when exposed to the network, and confidence in console security is often misplaced.
2. Basing access control on sheer trust—and trust alone—poses risks even behind a locked door and ignores the realities of the wide network exposure of remote console access—and what skilled professionals can do with it.

3. A lack of mainframe security knowledge among IT, security and audit professionals is itself a vulnerability.
4. Failure to address any of these issues exposes the enterprise to regulatory and business risks as well as security risks.

Misplaced Faith in the Security of the Console

Historically, console access has been secured by the isolation of physical access—yet even then, isolation has almost always been incomplete, since access to mainframe operational areas may be available to system programmers, managers, network staff, vendors, and even custodial employees. The introduction of remote console access, however, dramatically amplifies these exposures.

Putting the console on the network effectively removes the locked door and risks exposing console interaction to any traversed network. Console activity must therefore be highly resistant to discovery and exploit. This places much more responsibility for securing the console—and the mainframe resources for which the console is the gatekeeper—on the means used to enable remote access.

Most security or systems professionals are aware that some sort of encrypted tunneling capability is necessary to secure communications. Yet even there, incomplete knowledge of how secure tunnels actually function may open exploitable gaps in defense. For example, specific applications such as instant messaging often direct traffic *outside* a VPN, even when the VPN is configured to secure all traffic destined for external networks. Tools that secure mainframe console access must therefore be configured specifically for this purpose, making sure that gaps in network security do not threaten some of the enterprise's most sensitive communications.

Even undertakings as straightforward as authentication pose significant issues when applied to the mainframe console.

Even undertakings as straightforward as authentication pose significant issues when applied to the mainframe console. RACF operator authentication, for example, is difficult to implement on consoles and can make day-to-day operations onerous for technical staff. RACF authentication may also only prohibit making changes to the console. This has the disconcerting effect of leaving all console data visible, regardless whether a user is logged-in to the console or not. When console authentication is completely absent, the console itself may be exposed, which may lead to the exposure of mainframe data and critical functionality. Console access controls must therefore assure that the ability to reach the console at all is secured, well before the console itself is presented to a user.

Access Control Based on Trust Alone

When attackers seek to gain unauthorized access to a target, weak authentication is often the first and easiest avenue of exploit. Just as significant is the fact that highly privileged activity is often based on nothing more than a username and password. When there is little or no visibility or granular control in managing highly sensitive IT access, the enterprise may find that it has based its risk management strategy on trust alone.

Consider for example cases such as that of Roger Duronio, a one-time systems administrator at financial services giant UBS Paine Webber, convicted in 2006 of abusing administrative access to plant a "logic bomb" in critical corporate IT systems after what trial witnesses characterized as a dispute over compensation. Allegations in this case centered on malicious intent—but even more provocative is the case of Terry Childs. Once the administrator of the City of San Francisco's FiberWAN network, Childs was jailed in mid-2008 on multiple counts of computer tampering in the withholding of information needed to access administrative privileges, effectively locking the city out of its own infrastructure. Prosecutors claim that Childs went to substantial lengths to maintain sole control over this environment, allegedly to assure its reliability and performance and to protect it from the actions of administrators less knowledgeable or skilled than himself.

This highlights the fact that even a "well-intentioned" technologist poses a risk of lost control or damage—regardless whether these actions are intentional, as in the Childs case, or unintended. Just as important is the fact that even well-intentioned professionals can make mistakes. In fact, untraceable human error poses a risk not only to security, but to the availability, integrity and performance of critical information systems, and is not infrequently a root cause issue when IT problems appear in any environment.

These factors must be taken even more seriously with console access, in light of the mainframe's role as the custodian of the "crown jewels" of business information. Yet mainframe environments may be among the worst when it comes to access control based on trust alone. In more than a few cases, access facilities such as AF/Remote may never see a change in the default username or password, since changes could affect anyone and everyone that requires the facility for access. Once access is obtained, businesses may vary widely in the amount of visibility or control they deploy to monitor console activity or prevent console threats.

Lack of Mainframe Security Knowledge Is Itself a Vulnerability

Even though the mainframe houses some of the most critical business information assets, security professionals often do not have the mainframe expertise necessary to fully understand the unique risks and threats associated with that platform.

Even though the mainframe houses some of the most critical business information assets, security professionals often do not have the mainframe expertise necessary to fully understand the unique risks and threats associated with that platform.

The reasons for this have to do with how IT security has evolved, particularly in light of questionable assumptions that the mainframe is "inherently" secure. Many security professionals have come up through the ranks of networking, distributed, or—more recently—application environments, where threats have multiplied enormously. These issues demand the attention of security pros—but because the mainframe is often assumed to be more secure, security teams may not be as familiar with mainframe capabilities such as RACF, ACF2 or AF/Remote, or how to examine these facilities for vulnerabilities and risks unique to the mainframe environment. Of particular concern, these security professionals may not be aware of the added layer of security needed specifically to protect console access and the shortcomings of conventional security measures such as RACF in addressing these issues.

Compounding this issue is the apparent decline in the number of mainframe professionals with a working knowledge of z/OS security vulnerabilities. Such knowledge is critical to securing this high-priority environment. Despite this decline in mainframe expertise, businesses are responding to the current economic climate by extending investments in mainframe technology to cover areas like anywhere-anytime remote console access, integration in distributed application architectures, and platform virtualization. These trends expose the mainframe to more risk than ever—but without the expertise and tools needed to manage those risks, the exposure may be greater than realized.

Compliance and Business Risk Consequences of These Gaps

The fourth area of concern is a consequence of the other three: failure to address these issues realistically may expose the enterprise to regulatory penalties or business risks, as well as to security threats. Enterprises aware of these gaps may find themselves steering auditors away from too-close scrutiny of these issues, particularly mainframe console access and remote access—but one can reasonably expect that auditors will not turn a blind eye to these gaps for long.

The precedent has already been set in areas such as database audit, for example. For far too long, too many database deployments allowed risks such as default user accounts with widely known default access credentials to remain in place, unchanged. Today, database security is under substantially increased scrutiny because of the critical role the database plays in information risk control. It is only a matter of time before auditors become more aware of the issues that threaten the mainframe, because of the mainframe's critical role in managing sensitive information.

Already, compliance requirements such as the Payment Card Industry (PCI) Data Security Standard address issues such as authentication and access control, remote access, and network communications security.

- PCI Requirement 8 specifies a unique identity for each person with computer access.
- PCI Requirement 10 mandates the tracking and monitoring of access to network resources and cardholder data.
- Requirements 2 and 6 list multiple requirements for secure systems development and maintenance, changing default configurations, network security, and defining configuration standards.
- PCI Requirement 7 specifically addresses the restriction of privileged access, such as that afforded those who directly control IT functionality.

Other mandates such as the Sarbanes-Oxley Act ("SOX") and its global variants generally entail a control framework which, for IT, typically requires adequate separation of duties in accessing regulated information resources. Privacy regulation is particularly troublesome for many businesses, with multiple U.S. states and several nations imposing requirements that often overlap. Even if an organization has no facilities in a given jurisdiction, the availability of its services via the Internet may subject it to foreign or local regulation worldwide, whether the business knows it or not.

Even if an organization has no facilities in a given jurisdiction, the availability of its services via the Internet may subject it to foreign or local regulation worldwide, whether the business knows it or not.

Banks and financial institutions subject to these mandates are also among the most common mainframe users. As compliance requirements continue to grow and tighten and highly prescriptive measures such as PCI become more specific, one can hardly expect these mainframe deployments to be overlooked for long.

Closing the Gaps: The I/O Concepts Approach

As a leading vendor of secure console access and automation solutions for the enterprise, I/O Concepts recognizes these issues and offers actionable tools for tackling these risk gaps.

I/O Concepts' ioEnterprise Console Consolidation and Security (CCS) solution set extends console access via standard console connectivity hardware, including Open Systems Adapter-Integrated Console Controller (OSA-ICC) and Enterprise Systems Connection (ESCON) controllers, to Microsoft Windows, UNIX, Linux, and other non-mainframe environments. It enables multiple operators to manage multiple consoles simultaneously using standard protocols, without requiring modification to existing hardware or mainframe console definitions.

The ioEnterprise CCS solution also provides local and remote console access with integrated security measures that address the four areas of mainframe console risk, including capabilities for securing access to the Hardware Management Console (HMC). The product set provides security for network communications and flexible options for protecting and authenticating console access, even when multiple console sessions or consoles on multiple hosts are in play. Event management and audit capabilities are also available in the ioEnterprise CCS+ offering as well as in I/O Concepts' broader portfolio of event management products, providing visibility into risk events that help the enterprise monitor activity and help assure effective control. ioEnterprise also extends its functionality by integrating with existing Business Service Management (BSM) solutions that may not address the mainframe. As a solution purpose-built for the mainframe environment, it implements security measures that help administrators close knowledge gaps in mainframe security expertise.

Together, these capabilities help protect the business against compliance and business risks as well as security threats, providing more comprehensive control for the enterprise that recognizes the real risks of distributed console access.

Console Security in Any Environment

With consoles exposed by network access, enterprises must implement security measures to protect against threats in a wide variety of environments, and to recover the confidence lost when the locked door is no longer a factor.

The I/O Concepts' ioEnterprise Console Consolidation and Security (CCS) solution set adds a layer of security to console access, in accordance with best practices in "defense in depth," and has been evaluated to the satisfaction of I/O Concepts customers against accepted guidance including Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). The ioEnterprise CCS family isolates and separates console images based on security policy, such as read-only consoles that provide console visibility without the risk of unauthorized console access or use, command restriction, and customizable permissions.

Network communications are secured by industry-standard SSL encryption, while authentication can be flexibly supported at multiple levels depending on enterprise requirements. In the distributed environment, Microsoft Active Directory can be leveraged as a user identity resource, as can RACF, ACF2 or Top Secret for mainframe accounts. This allows greater flexibility in leveraging these resources, because they can be applied to console protection without interfering with the console itself. When more granular or independent access policy is required, I/O Concepts Password Authentication Server can not only authenticate access, it can also enforce password policies such as minimum number of characters or special characters, password expiry, or account lockout after a certain number of failed attempts.

These capabilities help to replace the locked door when they complement a best-practices approach to security in the distributed environment, extending console access with verifiable control wherever it may be required.

Replacing Trust with Granular Control and Visibility

When authentication enables access with much latitude in terms of privilege but little control over actions, access may be based on little more than trust. Yet when controls such as RACF are applied to the mainframe console directly, they may become an irritant if not an outright inhibitor—to operations staff, for example. Controls that work must fit as much as possible into the organization's accepted business processes, or they run the risk that authorized users as well as malicious parties will actively seek to circumvent them, actually *reducing* security through ineffective attempts to improve it.

*Controls that work must fit as much as possible into the organization's accepted business processes, or they run the risk that authorized users as well as malicious parties will actively seek to circumvent them, actually **reducing** security through ineffective attempts to improve it.*

The ioEnterprise CCS solution sharpens the scope of access without interfering with the privileges mainframe professionals need to work effectively. Role- and context-based access control can limit access to user name, group, role, location, and variables such as time of day. For example, one user may be allowed console access from any location within the enterprise network but not from external sites, while another may be restricted to access from a single device such as a specific desktop computer. These restrictions can also be applied to the command suppression capabilities available in the ioEnterprise CCS product family. For instance, one administrator may be allowed to shut down an LPAR, while another may not be allowed to enter such commands.

The alerting, reporting and event management capabilities of the ioEnterprise family expand visibility into what is done with console access once granted. The ioEnterprise solution can capture a record of every command issued in an ioEnterprise CCS console session, including attempts to execute suppressed commands. Event management capability can alert the enterprise when issues arise. It can also be configured to automate a response with custom-configurable commands that can deal with potential risks before they become a bigger problem.

While these capabilities may protect enterprises from potential or actual malicious activity, they also provide an important benefit in protecting the integrity of trustworthy professionals by documenting responsible actions. In addition, they offer the insight needed to troubleshoot problems when human actions are the root cause. This not only enhances problem resolution in mainframe management, it also supplements step-by-step documentation of proper procedures. Together, these values enhance mainframe reliability as well as security, reducing total risk.

Bridging the Gaps in Mainframe Security Expertise

Security professionals are charged with protecting the *whole* enterprise. This becomes a challenge when knowledge gaps exist that may result in security exposures.

This is an area where technology solutions can help close the gap, by implementing domain expertise that serves enterprise-wide security initiatives. This supports security professionals charged with securing the mainframe console, as well as mainframe experts who need flexible solutions for console access.

The ioEnterprise solution offers access security controls for the mainframe environment without requiring security professionals to be mainframe experts themselves.

The ioEnterprise solution offers access security controls for the mainframe environment without requiring security professionals to be mainframe experts themselves. It meets many security requirements for network communications security, authentication, highly granular policy-based control of access, a record of visibility into actions, as well as alerting, auditing and reporting capability that can be tuned as required to meet security priorities. At the same time, it helps the business extend greater flexibility to its mainframe personnel and operations. This provides a bridge between security professionals and mainframe experts that enables both to achieve their individual objectives while meeting common goals.

Reducing Compliance and Business Risks

By providing isolation of multiple console images, security for network communications, highly granular and flexible authentication, auditing, reporting and alerting capabilities, the ioEnterprise product set directly addresses many compliance gaps that may exist in mainframe environments. These are gaps that auditors can fully be expected to target, as compliance mandates continue to proliferate, and auditors dive deeper into more aspects of enterprise IT.

The ioEnterprise solution speaks, for example, to PCI Requirement 8, in providing multiple ways to specify a unique identity for each person with console access, as well as multiple requirements for network security and configuration control. It addresses Requirement 7 in restricting access to one of the most high-sensitivity environments in IT, and Requirement 10 for access auditing and event management.

The ioEnterprise solution also helps reduce business as well as compliance risks, by implementing the separation of duties in resource access that may be required under corporate governance mandates such as SOX. It secures and documents mainframe interaction that may be relevant not only to assuring data privacy, but to the protection of highly sensitive information critical to the business.

EMA Perspective

In the past, attackers and malicious parties were more focused on aspects of IT such as the network, because it was the medium that brought them into contact with targets of opportunity. Today, ubiquitous connectivity continues to expand the reach of threats as well as access. A global economy in turmoil only increases the risk, as attackers become increasingly desperate, and as market chaos opens gaps in risk control in entire economic sectors.

These factors make the mainframe a potential target of opportunity, not only because of its unique role as the custodian of highly sensitive information assets, but because of the gaps in risk control based on obsolete assumptions of mainframe security, poor access control based on trust, and inadequate mainframe security expertise. Given these gaps, it is only a matter of time before auditors as well as the malicious can be expected to find the chinks in the mainframe's armor.

When aligned with a best-practices approach to securing the distributed environment, the ioEnterprise CCS product set replaces physical and logical isolation with countermeasures for a wide range of access scenarios.

The ioEnterprise solution offers a proactive set of tools for addressing these issues, behind the locked door as well as in any network, public or private—*before* they become the subject of opportunistic attack, insider malfeasance, or a compliance defect report. When aligned with a best-practices approach to securing the distributed environment, the ioEnterprise CCS product set replaces physical and logical isolation with countermeasures for a wide range of access scenarios. It replaces blind trust with more sharply defined controls on access and visibility into activity. It implements mainframe-specific security that helps to close knowledge gaps between security and mainframe professionals.

Most importantly, it proactively addresses these issues before they become tomorrow's headlines, providing the protection needed for the crown jewels of business information systems, and helping security and compliance teams eliminate a target of opportunity before the malicious—and auditors—know it's there.

About I/O Concepts

I/O Concepts helps today's networked enterprise implement expert management and security solutions for their mainframe and midrange systems in order to facilitate more responsive, accessible and protected data center operations.

Since 1989, I/O Concepts has been providing expert solutions to help IT operations consolidate, secure, remotely access and monitor their mainframe and midrange data centers. The ioEnterprise solutions from I/O Concepts allows companies to protect their mainframe environment at the console level, consolidate data centers across the world, and more effectively monitor the mainframe/midrange environment with integrated event management, secure remote access and automation tools.

I/O Concepts is headquartered in Bellevue, WA and supports IT operations for some of the largest companies in the world. ioEnterprise solutions can be implemented quickly and I/O Concepts consistently helps its customers achieve immediate and identifiable cost savings and productivity enhancements. Learn more at www.ioconcepts.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst and consulting firm dedicated to the IT management market. The firm provides IT vendors and enterprise IT professionals with objective insight into the real-world business value of long-established and emerging technologies, ranging from security, storage and IT Service Management (ITSM) to the Configuration Management Database (CMDB), virtualization and service-oriented architecture (SOA). Even with its rapid growth, EMA has never lost sight of the client, and continues to offer personalized support and convenient access to its analysts. For more information on the firm's extensive library of IT management research, free online IT Management Solutions Center and IT consulting offerings, visit www.enterprisemanagement.com.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

1661.111308