

IBM @server zSeries
April 2004



**Securing Your Business
with the IBM @server zSeries**

Contents

2	<i>Introduction</i>
2	<i>zSeries server security strategy</i>
3	<i>Built-in security features</i>
4	<i>Security-rich virtual servers</i>
5	<i>Cryptography for highly secure transactions</i>
7	<i>Virtual Private Networks</i>
7	<i>Security from intrusion</i>
8	<i>Security features across the enterprise</i>
9	<i>Summary</i>

Introduction

Companies can lose billions of dollars every year to security breaches. Wise companies will take the time to invest now, working to secure their business with the goal of saving themselves trouble—and money—down the road. They take the right measures to provide a security-rich infrastructure because the cost of *not* doing so is high.

What does security mean to your company? It should mean:

- *Protecting it from intrusions*
- *Enabling secure financial transactions*
- *Providing a security-rich environment for Web commerce*
- *Ensuring stringent access control for resources that requires appropriate authorization*

IBM @server® zSeries® can help you on all of these fronts.

zSeries server security strategy

Since zSeries customers are some of the largest and most security-sensitive companies in the world, security has always been an important component of the zSeries strategy. Security is a key design point for zSeries servers, operating systems, middleware and applications. With the advent of e-business, zSeries has evolved to extend this robust security to the security needs of e-business today and with an eye toward the future.

zSeries servers have implemented leading-edge technologies such as high-performance cryptography, large-scale digital certificate support, Secure Sockets Layer (SSL) performance and advanced resource access control function. With Intrusion Detection Services, zSeries has enhanced its ability to help resist network-based attacks while embodying industry and international standards.

With the introduction of Linux to zSeries products, many zSeries server security features can now be extended to benefit these new virtual images on zSeries servers, particularly when it comes to highly secure partitions and high-performance cryptography. In January 2004, SUSE LINUX Enterprise Server 8 with Service Pack 3 on IBM eServer zSeries achieved Controlled Access Protection Profile compliance under The Common Criteria for Information Security Evaluation (CC), commonly referred to as CAPP/EAL3.

The zSeries server is at the heart of many customers' e-business, creating a need for interoperability with a variety of other servers. Numerous security applications and tools are available from IBM and other software vendors that enable zSeries products to participate in cross-platform security and to simplify security management.

Built-in security features

z/OS[®], the flagship operating system of zSeries servers, provides a robust security environment for your applications. Designed to balance multiple business-critical workloads on a single image, z/OS offers strong integrity between workloads via its multiple virtual address space design. System-level security options can provide flexible isolation among users and applications within a single z/OS image.

In addition, z/OS includes application interfaces for various external security managers such as IBM Resource Access Control Facility (RACF[®]), which can be used to identify and authenticate users, and to control access to and audit the use of system resources. Unlike some platforms in which the applications must perform a large part of the security processing, most z/OS applications only need to invoke the desired security services. z/OS provides security functions for traditional batch and online applications, as well as for new applications written using C/C++ and/or Java[™] Enterprise Java Beans. z/OS can identify and authenticate users using a variety of mechanisms, such as USER ID and password or digital certificates.

Multilevel Security Support

With z/OS 1.5 and IBM DB2 Universal Database[™] for z/OS version 8, IBM now provides multilevel security support on the zSeries mainframe. This can help meet the stringent security requirements of government agencies and financial institutions, and can help open up new options for e-hosting facilities. Multilevel security technology allows IT administrators to give users access to information based on their need to know, or clearance level. It is designed to prevent individuals from accessing unauthorized information and to prevent individuals from declassifying information.

With multilevel security support in z/OS 1.5 and DB2® v8, customers can enable a single repository of data to be managed at the row level and accessed by individuals based on their need to know. For example, a person with a top secret clearance can be enabled to access more information in a database than someone without the same clearance level.

Multilevel security addresses government requirements for highly secure data which can be shared between agencies on demand. While multilevel security began as a government requirement, its applications in general business sectors have now become apparent as security controls become more critical in emerging on demand, virtual environments.

Based on this multilevel security technology, z/OS 1.6 with the RACF optional feature is in evaluation for Common Criteria certification to the Labeled Security Protection Profile (LSPP) at EAL3+. Evaluation for certification to Controlled Access Protection Profile (CAPP) at EAL3+ is also in progress.

Security-rich virtual servers

zSeries servers can be an essential building block for server consolidation and the integration of e-business applications and traditional workloads. Multiple images of z/OS and hundreds of Linux images can run on a single zSeries server with the integrity and security for your mission-critical workloads. The two zSeries features that provide this highly secure virtual server environment are logical partitioning (LPAR) and z/VM®.

zSeries LPAR is designed to prevent the flow of information among logical processor partitions, instead enabling highly secure isolation. As of March 2004, zSeries systems are the only servers in the world to have earned Common Criteria EAL5 certification for the security of their LPARs.

For decades, IBM customers in all industry sectors—not to mention IBM itself—have employed z/VM virtualization technology as a trusted, reliable, highly secure and robust platform for multi-user computing and for hosting multiple virtual servers. z/VM is specifically designed to maintain the integrity of the virtual machine environment at all times, providing a security-rich hosting platform for hundreds of Linux images. z/VM is also in evaluation for Common Criteria certification to the LSPP at EAL3+ and CAPP at EAL3+ with certification anticipated by the end of 2004.

The z/OS operating system provides the infrastructure to exploit the strengths of each cryptographic feature, handling tasks transparently.

zSeries servers provide the performance and scale you need to handle highly secure Web transactions. zSeries has focused on improving SSL encryption performance.

Cryptography for highly secure transactions

The best way to secure information over the Internet is to encrypt it. zSeries servers provide exceptional performance and function via cryptography coprocessors and accelerators that are individually specialized to address various encryption needs. The z/OS operating system is designed to provide the infrastructure to exploit the strengths of each cryptographic feature. The result? The performance advantages of hardware-assisted cryptography are readily available to applications via the cryptography interfaces of z/OS.

The zSeries Cryptographic Coprocessor Facility (CCF) and PCI Cryptographic Coprocessor (PCICC) both have tamper-proof designs and support high-speed triple DES (TDES) encryption, as well as symmetric and asymmetric encryption.

One focus area for zSeries has been encryption hardware certification. As encryption has become a key security tool, industry and country requirements have driven IBM to provide or work toward these certifications. It is worth noting that IBM PCICC has earned the FIPS 140-1 Level 4 certification required by US government agencies. This certification gives customers confidence that their core encryption keys are designed to prevent capture by a hacker or even an internal systems programmer.

Both the IBM eServer™ zSeries 890 and 990 offer the PCI Cryptographic Coprocessor (PCIXCC), a replacement for the PCICC and the CMOS Cryptographic Coprocessor Facility that were available on the IBM eServer zSeries 900 and 800. In addition, PCIXCC implements the functions on the CMOS Cryptographic Coprocessor Facility used by known applications. PCIXCC supports security-rich cryptographic functions, use of secure encrypted key values and user-defined extensions--and it is also supported on the IBM z990.

SSL and security-rich Web commerce SSL is a public key cryptography-based extension to TCP/IP networking. For an example of the importance of SSL authentication, let's consider a Web commerce application that requests a customer's credit card number. The customer expects that the application is legitimate and not an impostor stealing credit card numbers. SSL provides this very function, helping to ensure private communications between parties on the Internet with the intent of allowing the credit card number to be passed from customer to marketing application without the threat of interception.

zSeries servers provide the performance and scale you need to handle highly secure Web transactions. zSeries has focused on improving SSL encryption performance, and it shows. For example, zSeries 990 servers offer speed, with capabilities of greater than 11,000 SSL handshakes/second with z/OS 1.4.¹ (To put that into some perspective, as recently as 1998, zSeries SSL performance was approximately 13 SSLs/second.) This ultra-fast and highly secure SSL comes courtesy of the zSeries server's optional PCI Cryptographic Accelerator (PCICA) features.

IBM has also extended cryptography support and enabled the PCICA feature on Integrated Facility for Linux (IFL) on zSeries models. IFLs are dedicated engines on zSeries servers for Linux workloads. PCICA support was previously made available for standard engines on zSeries servers running Linux. Linux (SUSE LINUX Enterprise Server 8) with PCICA encryption support achieved greater than 13,000 SSL handshakes/second on the z990.¹

Digital certificates

As digital certificates become increasingly important in securing transactions on the Internet—with capabilities that extend far beyond those of mere password protection—large enterprises are looking for a comprehensive and scalable solution to manage these certificates. The PKI infrastructure is the standard for public-key cryptographic security, which is used to help secure digital certificates and to manage their creation and use.

With the PKI infrastructure, digital certificates can provide trusted infrastructure for security-rich transactions over the Internet. As part of the Security Server element of z/OS, PKI Services for z/OS provides this infrastructure. PKI Services for z/OS combines PKI encryption technology with the z/OS qualities of service, including availability and scalability.

¹ The SSL rate was achieved with a z990 with 16 processors and 6 PCICA features (12 accelerator cards). These measurements are examples of the maximum transactions/second achieved in a lab environment with no other processing occurring and do not represent actual field measurements. Details available upon request.

IBM zSeries servers can help you manage your security facilities, whether you are protecting a single processor or a massive cross-platform network.

Virtual Private Networks

Companies can securely and cost-effectively extend the reach of their applications and data by creating a highly secure, private connection—a private tunnel. Many companies are replacing their existing telecommunications infrastructure with virtual private networks (VPN), implementing highly secure IP tunnels across the Internet between corporate sites as well as to business partners and remote users.

VPNs are specially configured, point-to-point networks. In addition to the security provided by this closed network, traffic can be encrypted. z/OS enhancements to Firewall Technologies provide Parallel Sysplex® cluster-wide security association support. This enables VPN security associations to be dynamically re-established on a backup processor in a Parallel Sysplex cluster when a Dynamic Virtual IP Address (DVIPA) takeover occurs. When the DVIPA give-back occurs, the security association will be re-established on the original processor in the Parallel Sysplex cluster. When used in conjunction with z/OS Communications Server's TCP/IP DVIPA takeover/give-back capability, this function provides customers with improved availability of IPSec security associations.

Security from intrusion

It's fair to say that all companies have some fear of being hacked by an inside or outside intruder. The consequences can be both immediate—the potential loss of customer data and the need to repair the hacked portion of your system—and long-term, in the form of damaged customer trust and loyalty.

z/OS, the robust operating system that is based on 64-bit z/Architecture™, delivers high qualities of service for enterprise transactions and data and extends these qualities to new applications using the latest software technologies. It provides a highly secure, scalable, high-performance base on which to deploy Internet- and Java-enabled applications, providing a comprehensive and diverse application execution environment.

z/OS is as “rock solid” as it's ever been, designed with improved protection against network-based attacks via:

- *Intrusion Detection Services that detect and take action*
- *IP packet filtering for controlled access*
- *Network address translation to hide internal IP address*

Although firewalls provide some level of protection against outside attacks, they can't help you when the attack is from within or when end-to-end encryption is employed. Host-based Intrusion Detection Services (IDS) complement network-based IDS sensors and scanners by providing defense mechanisms that can discard attacking packets before they cause damage, discard packets that exceed established thresholds and limit the number of connections from "greedy" users. In addition, IDS provides event recording and reporting.

Security features across the enterprise

To adequately manage your security infrastructure, you need to understand your enterprise's security needs and policies, and then obtain, configure and control the products and services necessary to implement those policies. IBM zSeries servers can help you manage your security facilities, whether you are protecting a single processor or a massive cross-platform network.

Because today's network environments are comprised of a complex group of systems and applications, a need to manage multiple user registries has been created. Dealing with multiple user registries can quickly snowball into a large administrative problem that affects users, administrators and application developers. Consequently, many companies are struggling to manage authentication and authorization for systems and applications. Enterprise Identity Mapping (EIM) is an IBM infrastructure technology that can allow administrators and application developers to address this problem more easily (and potentially at a lower cost) than previously thought possible.

zSeries servers can participate in centralized, policy-driven security authorization provided by the Tivoli® Access Manager, and z/OS can be part of the Tivoli secure-domain. z/OS can act as a network peer in receiving and maintaining security policy from a single point of administration. This support is ideal for customer environments that have complex security authorization needs that span multiple systems and platform technologies, including z/OS.

Summary

What does security mean to your company? Do you take the security of your systems and infrastructure as seriously as you should? Are you investing now to secure your business for the future?

If you protect your systems from intrusion, secure them to enable financial transactions and secure them for Web commerce, you can help save a lot of time and expense down the road. Best of all, with its many built-in security features, IBM @server zSeries is in a position to help you.



© Copyright IBM Corporation 2004

IBM Corporation
Integrated Marketing Communications,
Server Group
Route 100
Somers, NY 10589

Produced in the United States of America
04-04
All Rights Reserved.

IBM, IBM **@server**, IBM eServer, IBM logo, e-business logo, DB2, DB2 Universal Database, HiperSockets, Parallel Sysplex, RACF, S/390, Tivoli, z/Architecture, z/OS, z/VM, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

Information concerning non-IBM products was obtained from the suppliers of their products or their published announcements. Questions on the capabilities of the non-IBM products should be addressed with the suppliers.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

The IBM home page can be found on the Internet at **ibm.com**