

Technical Security Advantages of IBM System z9 and Virtualization on z/VM

Prepared for:
Gerald Araneo
IBM

By:
Sine Nomine Associates
43596 Blacksmith Square
Ashburn, VA 20147

April 2, 2007

Copyright © 2007 Sine Nomine Associates

All rights reserved.

Table of Contents

- 1 EXECUTIVE SUMMARY..... 4**
- 2 INTRODUCTION 5**
 - 2.1 Security Problem Overview5
 - 2.2 SMB Issues.....6
- 3 THE SYSTEM Z9 APPROACH AND THE Z/VM VIRTUALIZATION ENVIRONMENT 8**
 - 3.1 Security-Related Hardware Capabilities.....8
 - 3.2 Operating System Capabilities10
 - 3.3 Security Process Management Capabilities.....12
- 4 DISCUSSION CASES 14**
 - 4.1 Nexxar Group, Inc.14
 - 4.2 University of Toronto.....16
- 5 CONCLUSION 19**
- APPENDIX A – REFERENCES20**

1 Executive Summary

This article is part of a series illustrating the benefits of the IBM System z9 Business Class (BC) and z9 Enterprise Class (EC) servers for growth company environments. It focuses on the technical benefits brought to the data center by the IBM z9 in the areas of security and ease of management for security functionality. It specifically addresses the benefits of virtualization within the context of reducing migration risk.

It is intended primarily for data center technical managers, architects and administrators in growth company environments who are concerned with strengthening data security without impeding efficient access and speedy information flow to users. The audience to whom the paper is primarily addressed is expected to benefit most from a bias towards the System z9 BC, which is targeted specifically to the needs of customers who may not have previously considered their workloads appropriate to the mainframe.

This white paper is focused on the security benefits of virtualization on the IBM System z9 (BC) processors combined with the z/VM Operating System. This combination is an excellent platform for hosting hundreds of Linux images in virtual machines on a single System z, either as a stand-alone Linux consolidation server, or with Linux images on the same servers with the z/OS mainframe operating systems. (Note: this paper is not intended to address the z/OS aspects of security, which are well-documented in a wide variety of other IBM publications.)

Customers interviewed for this paper include Nexxar Group, Inc. and the University of Toronto. Nexxar, a financial services company in Europe, is an “early stage consolidator,” meaning its business model involves acquiring and integrating smaller firms. Nexxar has consolidated more than eighty x86 servers onto an IBM System z9 BC mainframe and, as a result, expects to save 30% per year in related operating costs. The University of Toronto is committed to being an international research university with 75 PhD programs and 17 professional faculties. Six Nobel Prize winners are among its graduates.

2 Introduction

Security and security management have been described as the largest modern “business killer” aspect of IT services design and implementation. The discussion in this paper examines some of the technical highlights of the overall IBM security strategy for the z9 Business Class systems, the strength of the virtualization solutions available on the platform, and how these systems can be applied to the problems that are prevalent in the small to medium-sized customer that may not be a traditional consumer of mainframe services. The paper also presents two technical viewpoints from users of the z9 BC, and some conclusions drawn from analysis of the IBM materials and field work with the security solutions provided by IBM.

2.1 Security Problem Overview

Regardless of the size of the enterprise, the technical problems surrounding security implementation revolve around three basic areas:

- Authorization - identify and manage roles and identities of a security object, the security entity may represent both human interaction with parts of the system, and/or program interaction with similar system components
- Access control - what is this security object permitted to view and/or manipulate, and how the relationships are defined and controlled
- Accounting - ensuring that actions taken by a security object can be audited and verified for correctness at a later date

Authorization requires the capability to generate and manage unique identifiers for individual user or application instances, and a way to rapidly modify and control these identifiers if compromised. Access control requires management of the relationship of objects, creating a complex matrix of objects, rules governing the interactions of objects with each other, and tools necessary to maintain the interaction definition. Historically, accounting has implied resource utilization information, but in a security context, it addresses both simple logging of events and more complex auditing requirements such as the evolving complex web of added industry requirements for compliance with specifications such as HIPPA regulations on health-related information in the United States, the comprehensive privacy and information protection statutes in the European Union, money laundering laws worldwide, and so forth.

Solutions to these three problems are a combination of *base* capabilities (delivered by the hardware, operating system and application infrastructure) and processes for *manipulating* the base capabilities to maintain a secure environment over time (no system can be considered to be secure without deliberate attention to maintaining security over time). Attention to the process management component of security is often overlooked in a discussion of security and security policy on a particular platform, both for maintenance of the system and the security entities within the system, and also the ability to validate that the desired policy is actually expressed/enforced by the equipment, and that the effects of the policy can be verified after the fact in a way that can be trusted.

Virtualization enhances the impact of the three issues discussed above by combining them (and the scope of their impact to a specific system image) within a single physical environment, introducing both intra-virtual machine requirements (the traditional application of security and

security policy), but also introducing the issue of control of security objects and resources outside of the scope of a single operating system's purview.

2.2 SMB Issues

SMB (Small and Medium-sized Business) customers, typically customers at the 100-1000 user range, are subject to all these problems, usually coupled with much more severe constraints on human and intellectual resources (personnel and the ability to understand and manage the security process) available to deliver and manage each aspect than larger organizations, while being subjected to the same management, auditing and reporting requirements overlaid on their larger brethren. When a SMB customer considers a security implementation or a possible platform switch, the evaluation of the environment for a SMB customer is often biased towards what fits the human and intellectual resources available and delivers the minimum capability to comply with external requirements, e.g. auditors and regulatory bodies.

Key factors in the decision and selection process for this customer type are delivered security capabilities at install, the tools available to define, express and implement security policies, and capabilities for monitoring and optimizing use of human and intellectual resources via automation and self-management, such as default logging setups that are familiar, trusted and usable for both internal tech staff and for auditing functions. The resulting impact on the business and technical components of the customer is the minimum possible business disruption consistent with the security requirements of the customer. This approach also impacts the discussion of virtualization in that the more capable the virtualization solution is in optimizing the basic delivery of security features, maintaining the security environment, and providing low-impact audit trails and logging, the more attractive the solution is to a SMB customer.

This combination of security skill requirements and automation also impacts the placing and management of the technology used in the environment. Part of the appeal of z/VM and Linux for the System z9 BC customer is the ability to leverage known skills and techniques brought from the discrete server world, enhancing the capabilities by adding the System z9 hardware functions and the z/VM isolation and virtualization capabilities on top of the basic operating system security capability. This idea of inheriting a good starting point based on familiar tools that can be *improved* by additional incremental investment in management tooling or personnel training is particularly compelling. This model enhances and extends the capabilities of existing human resources without demanding a complete overhaul of security management and management policy generation at each increment in complexity.

What IBM appears to be doing with this approach is to define an incremental and multi-layered approach to security and security policy management that will likely appeal to a SMB customer base. This kind of technical approach can be outlined as follows:

- Engineer native security and workload isolation capabilities at the hardware and operating system levels.
- Enhance application security capabilities by quickly leveraging platform capabilities via operating system or middleware interfaces as well as explicitly providing direct APIs to security features.
- Leverage management of shared capabilities (for example, the cryptographic coprocessor and accelerator in the System z9 hardware) to simplify management

- As skills and resources are available or additional requirements are placed on the environment, implement more sophisticated security capabilities by enhancing both the virtualization environment and implementing additional (e.g., z/OS.e or full z/OS) to get the most sophisticated security and transaction management capability for the System z9 hardware features).

The key interesting point for SMB customers is the ability to begin with a strong and well configured base and then evolving security management resources where necessary, without re-engineering the entire security management environment each time requirements change. This is difficult to accomplish in most discrete environments. The z9 has a compelling entry-level security basis for the SMB market.

3 The System z9 Approach and the z/VM Virtualization Environment

The next few sections of this paper explore some of the ways IBM has expressed this layered security design strategy in the System z9 and the z/VM virtualization solution.

3.1 Security-Related Hardware Capabilities

The System z9 BC adds a number of improved capabilities, including increased processor speeds and larger memory sizes, however many of the interesting components from a security perspective reflect a continuous evolution from previous models – primarily enhanced in the usability, capacity, and performance areas over their predecessors.

3.1.1 Logical Partitioning

LPARs (the ability to partition the hardware resources of the system into separate logical systems that maintain isolation from each other and are resistant to compromise from adjacent partitions via hardware-based enforcement capabilities) were originally introduced in the ESA/390 architecture systems in the late 1980s. With the current industry interest in virtualization and virtual systems, the long history of LPARs and the increased number of supported partitions (30 partitions on a System z9 BC) provides a solid base for mid-sized customers to separate workloads at a coarse level, allocating processor and memory resources to partitions while ensuring that applications cannot cross partition boundaries. Strict resource limits can be enforced, managing the ability to control denial of service or resource starvation attacks targeted against specific partitions.

Partitions permit both dedicated assignment and shared assignment of special purpose processors designed to enhance specific application functions, such as the IFL (Integrated Facility for Linux) processors for dedicated z/VM and Linux for System z workloads. IFL processors deliver full-speed performance at a significantly reduced price, even on entry-level systems where an administrative tradeoff of limiting general-purpose processor performance to gain reduced software licensing costs has been made.

This “always full speed” element allows implementation of complex encryption and authentication algorithms both within applications and in tandem with the embedded algorithmic support for selected cryptographic functions in the general-purpose processors via CPACF (Central Processor Assist for Cryptographic Functions – see below), and further enhanced for asymmetric algorithms (such as those used with the public key component of SSL transactions) and common commercial cryptographic operations (such as CVV code generation for credit card transactions) by use of the Crypto Express2 optional hardware feature.

3.1.2 CPACF

The CP Assist for Cryptographic Function (CPACF) feature for the System z9 processors provides 5 specialized machine instructions (as a group, these instructions are known as the Message Security Assist (MSA)) that support a set of symmetric cryptographic functions such as DES, TDES, AES-128, SHA1 and SHA-256, with a 'key in the clear' interface. These

cryptographic functions are aimed at encryption, decryption and hashing of data transferred over open networks and data sent to storage. The machine instructions for accessing CPACF function from user programs are described in the z/Architecture Principles of Operation (SA22-7832), and most System z9 operating systems provide higher-level access to the routines via an API.

3.1.3 Crypto Express2 Coprocessor/Accelerator

For applications which require encrypted keys, or acceleration of the algorithms commonly used in SSL transactions (such as asymmetric RSA public-key operations), up to 8 Crypto Express2 feature sets can be added to the z9 BC hardware. Each Crypto Express2 feature installs a pair of PCI-X-based cards in the z9 frame that can be configured in a coprocessor mode (for secure key encrypted transactions) or in an accelerator mode (for SSL acceleration). The addition of a Crypto Express2 feature provides a published rate of 6000 SSL transactions per feature (when used with z/OS) although there are no published numbers for use of the feature with Linux-based environments.

Both hardware security augmentation solutions are supported by z/VM and Linux for System z and System z9 to the extent that the presence of the hardware does not cause problems in normal operation and that the z/VM virtualization software is capable of virtualizing access to the security augmentation hardware, but some functions of the hardware have not been made accessible to these operating systems.

3.1.4 Certification by Accepted Independent Authorities (in Approved Configurations)

Addressing the simplification discussion in a different way, the ability to cite independent evaluation of a security solution by a disinterested third party is often an important step in evaluating the solution for the SMB customer. While this evaluation is limited to a specific “evaluated configuration” (which is often not reflected in the customer deployment), the certification provides a rapid evaluation check-box to establish that a basic secure configuration is possible using that solution. Two sets of evaluations that are commonly cited in auditing or evaluation circles as “minimum” requirements are the ISO /IEC 15408 Common Criteria evaluation, and the United States-originated FIPS.

3.1.4.1 Common Criteria

The Common Criteria is an international standard (ISO/IEC 15408) for computer security, describing a framework in which computer system users can *specify* their security requirements, vendors can then *implement* and/or make claims about the security attributes of their products. Testing laboratories *evaluate* the products to determine if they actually meet the claims, providing assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

Common Criteria evaluations are typically performed against a specific set of protection profiles which represent essentially specific classes of security devices such as network firewalls or encryption appliances used to provide digital signatures. Each profile specifies security requirements relevant to that specific application, and often are a template for product vendors to use in implementing a product intended for use in a particular area. The evaluating laboratory uses these profiles and a number of vendor-supplied specification documents, plus a rigorously applied and audited process of evaluating the profiles and documents, to evaluate the claim of

whether the device meets the claim of secure implementation – it covers both the validity of the claim and the rigor of the process used to validate the claim.

The rigor of the evaluations is assigned at one of 7 evaluation assurance levels (EALs). Each EAL corresponds to a package of assurance requirements which covers the complete development of a product, with a given level of strictness (EAL1 being the most basic (and therefore cheapest to implement and evaluate) and EAL7 being the most stringent (and most expensive)). While a higher EAL rating does not imply that the solution is more secure than a solution with a lower EAL rating, it does imply that the vendor has made significantly more comprehensive efforts to validate and test the suitability of the solution for a specific application – addressing directly the opportunity to simplify SMB deployment of the z9 BC for various purposes that require isolation, audit trails and requirements and encryption-related processing.

The z9 BC LPAR function has been evaluated at EAL5 (the full certification report is available online at <http://www.bsi.de/zertifiz/zert/reporte/0378a.pdf> and describes the testing and certification in extensive detail).

3.1.4.2 FIPS

The Federal Information Processing Standard (FIPS) publication 140-2 focuses more specifically on the implementation of specific cryptographic hardware and software that meet United States government requirements for use in government-sponsored activities and government-regulated industries such as healthcare and financial services that collect, store, transfer, share and disseminate "sensitive, but not classified" information. The FIPS publications coordinate the requirements and standards for cryptography modules which include both hardware and software components, and certificates which specify the exact module name, hardware, software, firmware, and/or applet version numbers are the result of the evaluation by United States and Canadian regulatory agencies.

FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4", addressing increasing requirements in 11 different areas, including manufacturing quality, key management and data path management, and tamper-resistance.

The resulting validation provided by the testing lab details the veracity of the vendor's claims and the suitability of the device for the intended purpose. The Crypto Express2 hardware security augmentation feature available in the z9 BC received FIPS 140-2 Level 4 certification on June 9, 2005

3.2 Operating System Capabilities

Once a stable foundation of hardware support for security functions is in place, the next step for the SMB customer is to evaluate how that support is supplied to the operating system and applications performing the work of the business. While some capabilities of the hardware are not yet exploitable from z/VM or Linux for System z, the hardware capabilities are augmented by additional functions in software to provide a richer security solution.

3.2.1 Isolation and Resource Management Capability in z/VM

Building on the partitioning capability of the System z9 hardware, z/VM provides even more granular control of workload by permitting additional isolation of workload with a logical

hardware partition. z/VM provides the ability to create and separate virtual machines (providing virtualized CPU, network and disk resources) to dedicate to applications or infrastructure, limited only by the physical resources assigned to the hardware partition containing the z/VM virtualization software. User identity and virtual machine configuration information is stored outside the normal filesystem areas and is tightly controlled via program interfaces. There is no direct access to this information from within an individual virtual machine.

Virtual machines can contain combinations of different System z9 operating systems simultaneously, providing common services and allowing rapid deployment and connectivity between virtual machines and external systems.

For the SMB customer, this capability offers the ability to separate and control the utilization of different types of workload – such as testing, development, and production work – on the same hardware at the same time. Development and test systems can be created on an as-needed basis by automated tools and eliminated after use, removing the possibility of using a unmanaged or ill-configured test system as a jumping-off point to a production system (as well as consuming no additional power, floor space, heating, or network connectivity).

3.2.2 Virtualization of Hardware Cryptographic Processors in Virtual Machines

z/VM allows the hardware security augmentation features to be virtualized in as many virtual machines as can be defined in the available system resources, dividing the performance of the hardware engine, but enabling the advanced features in any virtual machine which chooses to take advantage of the function. This ability, coupled with key management functions implemented outside a specific instance, provides a reason to provide enhanced security in all applications rather than a selected few applications.

Deployment of security augmentation devices is normally limited in the SMB space due to the high cost of deploying and managing devices in individual server instances. By simplifying the management of the hardware capabilities, and then making the augmentation capability directly available to any virtual machine, the number of support personnel and auditing complexity is minimized.

3.2.3 Linux Driver Support for Access to Cryptographic Processors

Once the hardware augmentation for security elements is enabled and presented within a virtual machine via z/VM's virtualization capabilities, Linux for System z also receives benefits from the System z9 environment. By using the OpenCryptoKi API interface, many of the CPACF features, and some of the Crypto Express2 functions are integrated into the OpenSSL software ubiquitously used in the Linux environment to perform cryptographic operations. For applications which do not employ OpenSSL, a device driver providing raw access to the cryptographic hardware and the OpenCryptoKi API library permit direct usage of the security augmentation hardware. Device driver code is provided by all the major Linux distributions for System z9.

Not all the functions of the Crypto Express2 hardware interfaces are exposed to Linux guests, however discussion with IBM and some publications indicate that work is ongoing in this area. This area benefits from the incremental implementation of complexity approach discussed earlier, as another System z9 operating system (such as a z/OS or z/OS.e operating system running in another partition or virtual machine) can be used to prime, enable and manage some additional

features that Linux may use without being directly conscious of the full protocol for configuring and operating the feature.

3.2.4 Evaluation of z/VM and Linux for System z Components by Independent Entities

Similar to the evaluation of the hardware logical partitioning cited above, the z/VM and Linux for System z operating systems have also been evaluated by external entities for Common Criteria certification.

A selected configuration of z/VM 5.1 has been awarded both a Controlled Access Protection Profile (CAPP) and the Labeled Security Protection Profile (LSPP) certification at the EAL3+ level in 2005, and SuSE Linux Enterprise Server 9 for System z has received a CAPP/EAL4+ certification. Other releases of both operating systems have been submitted for evaluation, but results were not available at the time of this paper.

For the technical designer in a medium sized environment, the certification of the operating systems as well as the hardware supporting the systems provides one more assurance that the overall environment can be built using secure building blocks in concert with good process management and control.

3.3 Security Process Management Capabilities

Building on the hardware and operating system capabilities, the z/VM and Linux environments offer access to a set of tools that address methods of managing the security process as well as the implementation of the basic function. The supported IBM (and 3rd party as well) tools concentrate on two areas: definition and configuration of security objects, and the management of the security process, both within the system and as part of a larger overall strategy.

3.3.1 Configuration and Definition Management

3.3.1.1 Directory Maintenance (DIRMAINT)

DIRMAINT provides the ability to create users and security identities within a z/VM system and controls how the z/VM system allocates system resources to those entities. DIRMAINT provides a menu-driven interface for new users, and a line-mode command interface suitable for program interaction when running in a authorized virtual machine.

3.3.1.2 RACF

Resource Access Control Facility (a subset of the eponymous utility available on other System z9 operating systems) provides the ability to define policies for how specific security entities and functions are used within a z/VM system. Using RACF, system administrators control the relationships between security entities, such as virtual machines ability to modify themselves or performance characteristics of their resource allocations. The z/VM implementation does not provide the external interfaces accessible to Linux or other guests, or some of the extended functions available in the z/OS RACF, however it can be integrated with a pre-existing RACF implementation to provide the basis for centrally managed and audited security implementation.

3.3.2 Tool Integration

3.3.2.1 DIRMAINT and RACF/VM Integration

Beginning with z/VM 5.2, IBM has linked the operation of DIRMAINT and RACF, coordinating the functions of the two management applications for the first time. This coordination provides automatic definition of security objects created by DIRMAINT in the RACF database and application of basic security profiles within RACF specifying how those security objects may be used. This capability is still in its infancy; however the step of coordinating the two applications forms a strong basis for building more sophisticated security process applications.

This framework for security management operations may be sufficient for SMB requirements; however, the evolution of the environment often demands a more coordinated approach with an existing security strategy brought from smaller discrete systems.

3.3.2.2 Incorporation of z/VM and Linux for System z into IBM Director

Complementing the DIRMAINT and RACF elements, the IBM Director application applies a higher-level set of knowledge to the capabilities of both the z/VM and Linux for System z environments. IBM Director provides a set of both management tools and a set of ITIL-based process “assistants” which provide both guidance and outlines of how to maintain a secure environment.

4 Discussion Cases

To illustrate the security advantages of IBM System z9 with z/VM virtualization, interviews were conducted with IT executives responsible for varying applications and deployment scenarios. The following sections describe the key attributes of the installations they manage, identify the systems they replaced and reflect the resulting benefits identified by the executives in their own words. Their comments are in italics. Wim de Ridder is Managing Director and CIO of Nexxar Group, Inc. Eugene Siciunas is Director, Computing & Networking Services at the University of Toronto.

4.1 Nexxar Group, Inc.

- **Server Consolidation and Security Authentication Framework**

“Security is always part of the discussion for the financial industry.” – Wim de Ridder

In 2003, Nexxar Group, Inc (a European financial services company providing services in more than 105 countries worldwide) embarked upon a strategy to accelerate growth through continued acquisitions. Critical to sustaining momentum of this growth without losing core management control was the ability to integrate the information processing requirements of each acquisition into a consistent and smooth running IT infrastructure. The largest outstanding technical issues resulting from the rapid growth and acquisitions were the disparate approaches to information security enforcement, and the problem of establishing a uniform model for secure access to information across potential institutional boundaries before, during, and after the mergers. Once a solution to those security issues was established, Nexxar was able to consolidate more than eighty x86 servers onto an IBM System z9 BC with virtualization via z/VM, and continues to move servers and applications into the framework at an accelerated pace – with the added benefit of enabling Nexxar’s IT organization to quickly create a secure, custom tailored computing environment for each “private label” relationship that utilizes a common – and commonly secured -- money transfer, money order, bill payment and check cashing services.

“The first step, of course, is to determine if any of the acquired computing environments are sustainable for where we want to go. The answer, unfortunately, has been no, not only from a scale, capacity and functionality perspective, but also security.” – Wim de Ridder

Before deciding to make the initial transition to its mainframe environment, Nexxar evaluated the IT capabilities of each acquisition. Nexxar found that its acquisitions operated different systems or flavors of systems frequently under different business models. Evaluations concluded that an integrated IT and authentication infrastructure had to be addressed that could support its products across many international environments, often with widely disparate regulatory and security requirements that are consistent with operating across national boundaries, even within supranationals such as the European Union.

Nexxar took two approaches to address the problem: one, to adapt existing infrastructure to a common set of security and system delivery services, and the other to evaluate new systems and vendors. In the first approach, the requirements were clear: as a financial services company, preservation of existing security of transactional data and the underlying metadata and information during the transition period present in an acquisition was paramount. Nexxar

anticipated that its applications would make extensive use of SSL and other encryption rich products via the System z crypto facilities on the mainframe.

“Security is always part of the discussion for the financial industry. Because the encryption capabilities are embedded in the (System z9) mainframe we only (need to) convert one element...it makes a big difference having cryptographic processes on the mainframe versus our distributed environment. Otherwise (in the distributed server environment) we would have to install certificates individually.” – Wim de Ridder

The evaluations resulted in a decision that the preservation of existing IT infrastructure was purely a transitional strategy, and new basic infrastructure designs and new security infrastructure was necessary. The selected architecture was a small System z9 BC supporting IBM WebSphere application server running on Linux for System z hosted using z/VM virtualization technology. Nexxar selected DB/2 to support data storage and management local to an individual WebSphere instance, and leveraged existing DB/2 infrastructure and security management for database in some small z/OS systems to support transactional processing in concert with the WebSphere front-end infrastructure.

The migration approach was to transition the security and authentication processing for each acquisition to the new infrastructure, then migrate applications into the new application environment and decommission the old equipment, updating technology and operations as part of the consolidation process. This two step process provides the ability to rapidly assimilate new acquisitions into the management framework in a way that can be audited and maintained, and then to support assimilation and management of new applications rapidly while maintaining a degree of individual system integrity and autonomy without compromising isolation between business units or the data that supports them.

The technical tools involved in the migrations include the integration of RACF with the Linux and WebSphere infrastructure via PAM access to RACF data, use of DIRMAINT and RACF for z/VM to propagate user and security data consistently to the virtualization solution, and leveraging the common security augmentation hardware tools of the z9 BC to support high performance encryption and SSL acceleration for all servers hosted on the z9 BC (a feature that was not supportable in a cost-effective manner in the distributed environment). The result of this initial step provided Nexxar the ability to consolidate six data centers to one and reduce the headcount required to operate its former x86 environment by 75%. The expected annual cost savings is 30%.

The second branch of Nexxar’s approach to its rapid growth and the diverse operating and regulatory environments in which it operates made validating and purchasing equipment less difficult across these environments. It was difficult to explain requirements to vendors in a straightforward year-by-year scenario. New acquisitions, products and applications together with the security demands of the locales in which they did business could not be precisely predicted.

“It is hard to get the attention of vendors when you start to explain your project by saying you are not set in the direction you are going. We noticed right at the first IBM stood out by giving us access to its different channels enabling us to compare its xSeries (Intel-based servers), pSeries (POWER architecture-based servers) and System z (mainframes) based upon our current environments and a set of variables for the future. This actually became our starting point. The comparisons were done in a two-step process. In the first step we looked at the kind of environment we would like to have. In the second step we did high level configuration pricing.” – Wim de Ridder

The consolidation of the server images into a single environment with robust external certifications and validations enhanced the ability to clear regulatory approvals in different jurisdictions, in addition to optimizing time and effort spent against addressing a multitude of distributed servers whenever an upgrade, audit or other necessary maintenance – a significant goal when one considers the cost of security patch maintenance against large numbers of Windows-based systems reflected in industry TCO studies circulated by other major pundits.

The consolidation technical discussion relies on the efficiency of the virtualization solution present in z/VM and the common security augmentation features of the z9 BC hardware. By offloading substantial amounts of the PKI and symmetric encryption operations to the CPACF and CryptoExpress2 hardware, the z9 BC can support comparable number of users as multiple Intel systems, and to provide high performance cryptography acceleration as part of the “standard” server infrastructure.

After evaluating a number of alternatives:

“It became clear that the System z was the preferable solution. We knew it was more expensive in the form of acquisition, but when you add in software and the required licenses in comparison to the number of processors, and that price was becoming very relevant, it was getting comparable to the solution we were looking for keeping the future in mind. Our goal is to share our infrastructures where we have a centralized form of control...that means virtualization where you don’t have to move memory, CPUs and physical servers. We found that virtualization on z/VM has been out there for many years with a proven track record. It allows us to set up a virtual environment with very secure production. It serves our need to rapidly provision private label functions such as purchasing transactions for other companies with dedicated segmentation of data, which is very easy to do in a virtual environment. For us, the data integrity and separation (security) guarantees we can give to our customers is a benefit of System z9.” – Wim de Ridder

Describing this to regulators has proven to be an added benefit as well.

“In conversations with the regulatory people as soon as we go into explaining the differences between our former distributed environment and System z, the ease of operation, how everything is centralized and controlled through RACF, the conversations are easier and everyone is aligned that it is a secure environment. In the distributed environment there are many elements to manage while with the mainframe we control everything through RACF.” – Wim de Ridder

4.2 University of Toronto

- **Upgrading to the System z9 BC from a System z800**

“You don’t have the threat or the opportunity for hackers to play with it or figure ways to break it.” – Eugene Siciunas

The University of Toronto selected the System z9 BC to upgrade from its former z/800 system supporting most student applications. The system runs student registration and a expanding range of course management applications related to student life in all parts of the university, such as student records and transcripts, course adds and drops, fees, and the all-important exam schedules and grade inquiries. Encountering spikes in demand at the start and end of each semester, the

University wanted to improve service to students and faculty as part of evolving both access to its long standing application infrastructure and security techniques used to protect and manage the information.. Many of these applications had been developed by the University over an extended period, and represent substantial investments in business logic and maintenance. The University also is engaged in a campaign to highlight a heightened public attitude toward information security, particularly the security of personal information. Canada's Freedom of Information and Protection of Privacy Act, while focused more on processes that determine what information can be sought, why, and controls over how it may be used reflects a regulatory requirement even within the university community. Previous to the z9 BC, institutional and personal data can find its way onto servers and personal computers that are subject to theft – and many published reports of potential harm to the individuals whose personal data has been compromised and negative publicity impacting the stature of the organization that lost the data. Robust and ubiquitous use of encryption methods are one way to protect information before it is physically at risk.

“The z9 could play a ever-larger role in (solving) this problem as we continue to explore its capabilities and figure out methods to extend the use of the cryptographic engine. We have it now so let's see what we can do with it. With regard to the privacy and disclosure issues, the risk is not just financial; it is also loss of reputation which is another reason why we are taking it seriously.” – Eugene Siciunas

The technical discussion around the z9BC and the addition of z/VM and Linux for System z revolved around preserving the existing security for personal data, and extending those protections to systems outside the mainframe arena. These problems (together with the Capacity on Demand function to address demand spikes during registration and add/drop periods), were the important decision factors for the University's Director of Computing and Network Services.

“We (had been) a z/OS shop supporting the administrative applications for years...the application was (originally) designed for MVS (and) we were not going to change it on a whim. We only made our previous (application) change because of Y2K pressures and prior to that it had been around for twenty or thirty years. So we don't take these changes lightly... the discussion around Linux and z/VM revolved around how we could provide augmented access management to the student records system without significant reengineering of the existing application as well as take advantage of a SecureID initiative being implemented in parallel. – Eugene Siciunas

The technical solution replaced the z/800 previously installed at the university and partitioned it into two components; a logical partition supporting the existing z/OS system and a logical partition supporting the SecureID initiative and the integration tools necessary to interact with the other systems on campus, both hosted on Linux for System z guests using z/VM virtualization to support multiple guest systems.

This approach allowed the University to enjoy the benefit of enhancing their existing practices so that no changes needed to be made to its security practices which included requirements for dual access using RSA SecurID® on selected applications and web access parameters for the more common user interactions.

“Rolling the System z9 into the University's existing framework was a snap. Just one weekend, unplug one and plug in the other. There was no problem at all. Also (the z9 BC) made it very affordable in that we could improve the student experience and not have to sell half of the University's buildings to do it. That's why we are in the z9 family.” – Eugene Siciunas

The applications in the Linux environment directly integrate with the overall SecureID infrastructure as any other client; no special processing is necessary. As the security models expand, the applications on z/OS will also begin to consult this infrastructure, constructing a common authentication and authorization model where the mainframe can both consult and provide security data and control information to a disparate set of clients and applications.

5 Conclusion

Based on these examples and the capabilities of the hardware, operating systems and management applications, the System z9 BC, z/VM and Linux for System z security story is interesting to SMB users as both an excellent starting point, and as part of an evolutionary solution. The approach of providing a strong native capability and implementing the control and management of that capability at multiple levels is attractive in that it provides a low implementation cost for a basic level of security, but enables additional layers to be added as the organization grows and evolves over time. The addition of virtualization to the mix also augments the ability to deliver a much more comprehensive capability – the idea of advanced security everywhere has always been limited by the management requirements of the complex hardware and software required – virtualization of common security augmentation hardware across the virtual environment makes that requirement significantly less onerous than any other similar environment.

Appendix A – References

Some materials above have been gathered by research on publicly available websites, including but not limited to the IBM web site. Resources used include:

The IBM website www.ibm.com

About Virtualization <http://www-euro3.ibm.com/systems/virtualization/about>

z/VM Overview <http://www.vm.ibm.com/overview>

IBM System z9 Business Class <http://www-03.ibm.com/systems/z/z9bc>

What IT Analysts Are Saying About The New IBM System z9 BC
<http://www-03.ibm.com/systems/z/about/quotes>

The New IBM System z9 <http://www-03.ibm.com/systems/z/feature042706>

Altmark, Alan and Laking, Cliff , z/VM Security and Integrity, April 2005

IBM System z cryptography for highly secure transactions <http://www-03.ibm.com/systems/z/security/cryptography.html>

Evaluation Assurance Level http://en.wikipedia.org/wiki/Evaluation_Assurance_Level

Common Criteria http://en.wikipedia.org/wiki/Common_Criteria

FIPS PUB 140-2 <http://csrc.nist.gov/cryptval/140-2.htm>

“The Brave New World of Mainframes”, *z/Journal*, October/November 2006, p. 38

