Today’s Mainframe:
The power of industry-leading security, the simplicity of centralized management

IBM System z servers: Security-rich by design

The phrase “don’t put all your eggs in one basket” was coined long before the advent of computers. When it comes to system security, however, today’s information technologists know that the more application and data “eggs” you have scattered about, the more vulnerable your system becomes to attack. That’s why it’s critical that your system security “basket” has the integrity and security qualities to protect both applications and data without the application logic being responsible for data security.

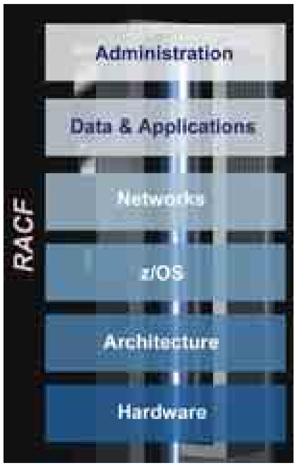
IBM Security Specialist Jack Jones says IBM System z™ mainframe servers provide the foundation for a solution by the very nature of their design. Jones says, “The System z operating system, z/OS®, evolved from the needs of a business environment in which several applications needed to concurrently share computing resources while maintaining the separation of applications. The operating system had to be isolated from the business applications and ensure that applications could not interfere with each other, or for that matter, tamper with the operating system. This perspective is important, as it’s a quality that was identified in the business environment and ingrained early in the evolution of what is now z/OS. This separation is the basis for system integrity and system security on the mainframe. Contrast this perspective with academic environments and lab settings where other operating systems such as UNIX® and Windows® evolved—one application per machine and with limited controls placed around sharing networked resources. These are two very different legacies with different system security implementations.”

What does this mean? The mainframe is a system that is designed to be rich in security features highly resilient to hacking and information theft because of the specific way in which the hardware and its microcode are implemented. This is what the designers of other operating systems have been challenged to do with the same level of effective integrity and isolation.

Security considerations come naturally to the designers of IBM’s Systems z. They have inherited an operating system that works in harmony with its own hardware since it does not have to be adaptable to running across multiple platforms. Yet z/OS allows for a large variety of applications, from UNIX applications to Java™ applications, that can utilize system security and interoperate with other applications running on the platform in a highly secure fashion for a complete business solution. As Jones puts it, “As z/OS has extended its influence across the enterprise, interacting with other platforms and servers, z/OS security has kept pace with advanced security function such as Public Key Infrastructure and networking intrusion defense support, plus much more. Along this path, z/OS security has continued to be guided by the principles that were established when the evolution began in the 1960s.”

The way System z technology works is that each time an application tries to run, it has allocated a certain amount of computer resource called an address space. With technologies such as storage protection keys, the application has no way of directly accessing data or another address space. The application goes through the z/OS operating system to gain access to any of these resources, and z/OS can verify whether the application is in fact authorized to access the data. If the application is authorized, it does not retrieve the requested data directly but instead receives the data from Resource Managers, which are elements of the operating system that ferry data between the application and its stored location. When properly installed and configured, it is nearly impossible for an application to make changes in another application or the operating system itself without it first going through the security and integrity features of the System z hardware and the z/OS operating system.

IBM RACF® (Resource Access Control Facility) is the security component that can be installed as part of the z/OS operating system. The administrator of the customer's system determines policies and settings to be configured in RACF, such as which users are registered to access what applications and which resources each application is allowed to use. Whenever there is an attempt to retrieve data, the Resource Manager checks with RACF before retrieving information for the application that requested it. The z/OS System Integrity Statement, which IBM first issued in 1973 and still adheres to, assures us that if the customers use RACF and the z/OS security infrastructure, z/OS will ask the appropriate security questions and write the appropriate audit records when resource accesses are attempted. In recent years, a HealthChecker has been added that monitors critical aspects of the security environment and provides an alert when high standards of security are not being maintained. With this arrangement, the customer is provided with automatic help in taking precautions against outside threats.



In short, applications and data benefit from the intrinsic security and integrity that is provided by System z. These limit the ability for applications that are not trusted to access another application's data. Built on this architecture and foundation, the z/OS operating system and the z/OS security manager, RACF enables differing policies to facilitate the controlled sharing of data—and the security admin may classify both applications and data with compartment labels—a measure of the sensitivity of the application and data. This sort of flexibility is important when considering legislation and business requirements that govern how data is being used. Other operating systems may mimic z/OS operations and terminology, but they cannot match the advantage that z/OS and System z hardware have in working in a collaborative fashion to create a security-rich environment.

Such fundamental differences are able to make System z mainframes less susceptible to the work of computer hackers. For instance, one typical hacker attempt to enter a system is known as the "Buffer Overflow Attack." In most operating systems, applications consist of memory stacks, which have data at the top and executable instructions at the bottom. In a Buffer Overflow Attack, a hacker simply has to fill up the data portion of the application's stack, and it will allow him to write anything he wants into the executable portion, thereby taking control of the application. z/OS works differently. In System z mainframes, all applications are kept in large sections of their own address space. When a datum has to be used, it is taken out of the blocks of "virtual storage" and moved into "real storage," where it can be manipulated—but only by someone with the correct Storage Protect Key, and nobody else. This combination of virtual storage and storage protect keys allows z/OS to follow the requirements of the logical stack concept that UNIX and TCP/IP requires but in the implementation the data portion and the executable portion of the stack are isolated.

With data broken into blocks and each block guarded by another level of security, an invading hacker has little chance of altering the system. The difficulty is compounded by the fact that System z developers routinely conduct penetration testing during the development and verification processes in an effort to make the system is as impregnable as can be foreseen.

IBM System z Security Initiative Leader Mary Moore says, "The System z team keeps up to date on new developments in hacker techniques, constantly testing and re-testing the system to make sure even the newest methods of computer trespassing are challenged. As further protection, they integrate software elements such as intrusion defense and rigid audit trails into z/OS, which can help minimize the amount of damage that may be caused an attempted security breach."

Even as they take advantage of the opportunities that the System z development history has afforded them, the developers of the technology work constantly to make sure their product compatible with new developments in IT and systems security. The result is a product that is steadily enriched in its security. The system that has been improved in countless versions over four decades forms a basis for technology that is constantly growing in the size of the workload it can handle, while it gradually shrinks in the number of operations staff and security administrators that are needed to support it.

Operations staff however, does play a vital role in maintaining the striking differences that set System z products ahead of their competitors. Open source technologies such as Linux® have become an economical alternative for some companies in recent years. However, the very fact that their source code is entirely open does not alleviate the need for service and support. A System z client can always call IBM to get help. As Jones explains it, “If I find a problem on z/OS, I pick up a phone and I call IBM, I talk to somebody, once they discover a problem, we fix it, then we go back and re-test the environment before we’ll put it out and make sure that it goes out to the customers.”

New security features are routinely incorporated into each year’s edition of z/OS, which usually makes its debut circa September. Each release goes through a two-to-three year period of development and multiple phases of verification, since while one release is being finished and tested before its distribution to System z customers, the following one is already being planned with further improvements, new and enhanced capabilities. In this way, the company is able to steadily and constantly continue developing its product, while at the same time providing to customers a series of sequential release versions. Jones explains, “We go through development and multiple testing cycles, and we do as much testing as we can before we get it out. Any new hacking tool or little scripts that the research and development folks have discovered will hit up against our new version of the operating system before they ever release the code itself to a customer. So we try to make it as secure as possible before we even let it out the door.”

This kind of security has been a hallmark of System z products for many years—since 1973, in fact, when the first version of the z/OS (then “MVS”) System Integrity Statement was made. The manufacturers of this technology know that security must not only be strong and reliable but also pliable to the special needs of every individual customer. That’s why the settings of RACF are always determined by the client and are not set elements of z/OS. As Jones explains, “It’s a partnership. This Integrity Statement essentially says we can do all this stuff from the operating system side and from the hardware side we can maintain our environment and we can make sure that the customer’s security policy is followed the way that you want it to be followed. However, you, Mr. Customer, are going to have to make sure that your security policy is correct.” In recent years, IBM had backed this z/OS System Integrity Statement by having System z and z/OS with its RACF security component certified by the Common Criteria at the very high level of EAL 4+ for both Controlled Access Protection Profile and Labeled Security Protection Profile.

With the unique hardware engineering of System z mainframes and the z/OS operating system, combined with the flexible and customer tailor able security capabilities, a customer who chooses to invest in System z mainframes is provided with both freedom and safety. It’s a combination that has served both System z and its users well over the technology’s forty-odd-year history, and as Jack Jones reminds us, “It’s really that history that makes the difference.”

IBM Systems Group
Route 100
Somers, NY 10589
U.S.A

Produced in the United States of America
April 2007

References in this publication to IBM products or services do not imply that IBM intends to make them available in every country in which IBM operates. Consult your local IBM business contact for information on the products, features and services available in your area.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply. Photographs shown are of engineering prototypes. Changes may be incorporated in production models.

This equipment is subject to all applicable FCC rules and will comply with them upon delivery.

Information concerning non-IBM products was obtained from the suppliers of those products. Questions concerning those products should be directed to suppliers.

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