SECURITY BENEFITS OF RED HAT ENTERPRISE LINUX 5 ON IBM SYSTEM Z

By Karl Wirth, Red Hat and Peter Spera, IBM Corp.

ABSTRACT
For decades, IBM mainframes have been the hardware platform of choice for secure computing. IBM System z builds on and extends this tradition. Red Hat® Enterprise Linux® has been designed by, and for, the most security-conscious organizations in the world. Red Hat Enterprise Linux 5 provides top-of-the-line security in a mainstream, open-source operating system. Working together, IBM and Red Hat have created a compelling solution for security—Red Hat Enterprise Linux 5 on IBM System z.

This paper will explore the security benefits of Red Hat Enterprise Linux 5 on IBM System z.
SECURITY BENEFITS OF IBM SYSTEM Z

PHYSICAL SECURITY
Physical security is a critical component of any security policy and an essential security benefit of a mainframe. Hundreds of boxes spread throughout an organization can introduce risk and complexity. The organization can be difficult to protect, both physically and logically. System z provides Logical Partitioning (LPAR) and z/VM on the mainframe to permit multiple images to reside side by side in the mainframe environment. These technologies provide the isolation required by enterprise and government customers in a Common Criteria certified environment. It is much simpler to protect one or several System z machines located in the core data center.

The vulnerable and exposed networking configurations deployed in the distributed environment can be duplicated within the physically secure mainframe environment, adding the benefit of physical security and the ease of auditing the network deployment.

VIRTUALIZATION
The benefits of this physical security would be of little use if all of the applications consolidated onto the mainframe were run together in one logical image. For decades, IBM mainframes have been providing virtualization functionality. On System z, LPAR can be used to carve the massive mainframe resources into partitions that better represent the workload requirements. Within an LPAR, z/VM enables a large number of operating system images with diverse or associated applications to run simultaneously on the same machine, while maintaining the isolation of each image. Leveraging HiperSockets, System z allows physically secure high-speed communication across images residing in separate LPARs.

AUDIT
Red Hat Enterprise Linux 5, along with IBM’s System z, provides the high level of auditing capability required by the most discerning customers. From the auditing capability integrated by Red Hat to the auditing capabilities of the mainframe (including LPAR, z/VM and networking connections), organizations can get the information they need to ensure their security policy is soundly deployed.
Security benefits of Red Hat Enterprise Linux 5

Platform security must be a pervasive and fundamental part of the platform—not just an add-on. It must be continually reviewed and maintained to ensure platform integrity. It must organically include the partner ecosystem and the larger platform community. For these reasons, Red Hat Enterprise Linux 5 stands out as a state-of-the-art, industry-leading choice for settings where security really matters. Four values define the Red Hat approach:

• Innovation. Red Hat leads the way in developing new security technology for Linux, from SE Linux and EAL 4+ certification (both described in the next section) to attack protection (detailed below). Plus the many additional innovations described in the Red Hat Enterprise Linux resource center: http://www.redhat.com/rhel/resource_center/

• Transparency. The availability of the source code for Red Hat Enterprise Linux makes it a better alternative for creating secure systems than proprietary code. The innovations in Red Hat Enterprise Linux 5 are due in no small part to the power of the open source development model, which combines the input of customers, partners, developers, end-users, and administrators.

• Vigilance. Red Hat continually looks for potential security exposures, certifying each package and delivering tested security updates through Red Hat Network. Customers can further strengthen their infrastructure through Red Hat services and support.

• Inclusiveness. Red Hat works closely with partners like IBM to make sure customers have choices when building a secure, integrated environment.

Red Hat Enterprise Linux 5 includes four major innovations that protect systems against attack, particularly in the area of buffer overflow and other memory-based attacks. These new features are:

• Fortify source. This check is now run on all selected packages. When the compiler knows the size of a buffer, it is possible to ensure the buffer will not overflow.

• Stack smashing protection (canary values). The system will place a canary value at a randomized point above the stack. This canary value is verified during normal operation. If the stack has been smashed, the canary value will have been overwritten, indicating that the stack has indeed been smashed. This method can detect buffer overflows early.

• Pointer encryption. Function pointers are encrypted with unique random values. This is intended to detect an overwrite of a pointer in memory and prevent the subsequent redirect of execution.

• SELinux memory protection. This enhancement can prevent any memory that was writable from becoming executable. This prevents an attacker from writing his code into memory and then executing it.

At Red Hat, the values of innovation, transparency, vigilance, and inclusiveness are not mere words, but business processes that produce and maintain the most secure product possible, while delivering the best value to customers. That’s why Red Hat has consistently topped the CIO Insight Survey during the last three years.
The Red Hat Enterprise Linux 5 System z solution brings an organization the following additional security benefits.

**ONE LINUX ACROSS THE ENTERPRISE, END-TO-END**
Red Hat’s commitment to a unified code base means that Red Hat uses the same source code to deliver Red Hat Enterprise Linux on IBM System z as it does on an x86 platform. Stable, predictable mainstream Linux code for your mainframe environment and quicker resolution of security vulnerabilities. The same system administrators can run Red Hat Enterprise Linux on System z as they do on other platforms. Their expertise brings increased skill and accuracy, quicker response time, and greater overall enterprise security.

**SUPPORT FOR SECURITY ENHANCED LINUX**
Unique to Red Hat Enterprise Linux, Security Enhanced Linux (SELinux) provides granular policy-based control over programs’ access to data and kernel resources, preventing a compromised program from acting outside its policy.

SELinux was developed in coordination with the open source community and the National Security Agency to provide the highest levels of security for the Linux operating system. SELinux is not a separate Linux distribution or branch. Rather, it is a feature of Red Hat Enterprise Linux.

By default, over 200 core system services in Red Hat Enterprise Linux 5 are protected by targeted policies. So organizations can quickly benefit from the security provided by SELinux.

As an added benefit, Red Hat Enterprise Linux 5 also includes enhanced SELinux management tools that simplify the process of creating, customizing, managing, and troubleshooting SELinux policy.

**COMMON CRITERIA EAL4+ CERTIFICATION UNDER CAPP, RBAC, LSPP ON SYSTEM Z**
Red Hat Enterprise Linux 5 is the first Linux operating system to ship with native support for the functionality necessary to meet Common Criteria for Trusted Operating Systems. This includes all functionality to enable EAL 4+ certification under the following protection profiles: CAPP (Controlled Access Protection Profile), RBAC (Role Based Access Control), and LSPP (Labeled Security Protection Profile).

In addition to the Common Criteria certifications already available to customers of System z, IBM is sponsoring the EAL 4+ certification of Red Hat Enterprise Linux 5 on System z. The existing certifications, which include LSPP on z/VM and z/OS, combined with the Red Hat Enterprise Linux 5 certification, provide a secure platform environment capable of meeting the most stringent public or private sector security policies.

For customers outside of the government, this provides assurance that the platform is designed, reviewed, and tested to the government’s most rigorous security standards.

For government customers required to run Common Criteria for Trusted Operating Systems, Red Hat Enterprise Linux 5 provides an open source solution that natively
supports multi-level security. This is an exciting mainstream option for customers realizing the benefits of the open source operating environment and consolidation on IBM's System z.

VIRTUALIZATION
UIBM's z/VM provides the security benefits of a historically proven virtualization environment for Red Hat Enterprise Linux on System z. Multiple Linux images can safely run side by side within the z/VM environment. These images can be entirely isolated or part of a bigger multi-image end-to-end solution. Networking between images can be implemented via virtual LANs and switches to provide the flexibility needed by any end-to-end enterprise solution. If a minimal number of images are required, LPAR could be considered as an alternative to z/VM; however, when used in conjunction they provide a highly configurable, extremely flexible alternative for running Red Hat Enterprise Linux and its workloads.

CRYPTOGRAPHIC ACCELERATION
Cryptographic functions needed to protect data, validate endpoints, or sign are vital to any secure application deployment, but they can be CPU-intensive when implemented in software. System z includes cryptographic instructions, SSL accelerators and secure tamper-sensing/tamper-responding hardware cryptographic coprocessors of which Red Hat Enterprise Linux can take advantage. These options give applications and enterprises the security, flexibility, and speed they need to meet the demands of today's end-to-end enterprise security requirements.

IBM System z supports two approaches to key deployment, Secure Key and Clear Key. A Secure Key is a key that is encrypted under another key within the boundaries of the secure hardware environment. While the encrypted version of that Secure Key may leave the hardware environment, the clear value of that key is never available outside the secure hardware environment. Secure Keys and secure key functions are most often used by banking and finance applications. A Clear Key is a similar cryptographic key, but it is not encrypted under another key. Thus, cryptographic functions are quicker to perform with a Clear Key. The most pervasive example of Clear Key cryptography is the negotiation that takes place to enable an SSL-protected transaction. Internet users enlist their web browser to connect to a store's server and order products via an SSL-protected transaction.

Running Red Hat Enterprise Linux on System z will allow your organization to take advantage of the following cryptographic functions for added security and performance:

1. Clear Key RSA accelerator cards, as well as symmetric crypto and hash functions based on built-in hardware instructions for AES-128, DES, TDES, SHA-1, and SHA-256 are available with RHEL 5
2. Secure Key-based crypto hardware features are planned and will be supported in a future release.
3. Kernel crypto API support is planned and will be supported in a future release. This will allow crypto API calls from the kernel to, without modification, leverage the System z hardware crypto hardware instructions.
CENTRALIZED AUTHENTICATION

UIBM's z/VM provides the security benefits of a historically proven virtualization environment for Red Hat Enterprise Linux on System z. Multiple Linux images can safely run side by side within the z/VM environment. These images can be entirely isolated or part of a bigger multi-image end-to-end solution. Networking between images can be implemented via virtual LANs and switches to provide the flexibility needed by any end-to-end enterprise solution. If a minimal number of images are required, LPAR could be considered as an alternative to z/VM; however, when used in conjunction they provide a highly configurable, extremely flexible alternative for running Red Hat Enterprise Linux and its workloads.

SUMMARY

For enterprise and government organizations, Red Hat Enterprise Linux 5 on IBM System z provides significant security benefits. System z provides robust physical security, virtualization, hardware cryptographic acceleration, and audit capabilities. Red Hat Enterprise Linux 5 combines an innovative, transparent, vigilant, and inclusive approach to security with a wide variety of features that protect systems against attack, particularly in the area of buffer overflow and other memory-based attacks. Red Hat Enterprise Linux 5 on System z gives organizations one Linux architecture across the enterprise, support for Security Enhanced Linux, a Common Criteria EAL4+ certification under CAPP, RBAC, and LSPP, cryptographic acceleration, and centralized authentication.