Information Technology Company

Key Resources, Inc. Enforces IBM® z/OS® Statement of Integrity with ITC's uPDT™

case study

For almost 40 years, a foundation of mainframe computing has been IBM's Statement of Integrity (SoI).

First issued for MVS™ and updated for OS/390® and z/OS, it defines and demonstrates IBM's on-going confidence in and commitment to enterprise-class systems, most recently refreshed as the zEnterprise™. This longstanding and very public SoI is a critical distinction between z/OS and other computing platforms.

This commitment mandates design and development practices that prevent unauthorized application programs, subsystems, and users from bypassing formal z/OS interfaces and therefore circumventing z/OS security — that is, gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless legitimately permitted. When system integrity problems are reported, IBM resolves them.

But the world has changed — for better and worse — since the mainframe's inception and centralized computing services. Now, security breaches can be created anywhere and discovered or triggered by an employee. Vulnerabilities are often inadvertently created by developers through programming techniques that speed development or are designed without considering system integrity.

Sadly, though, mainframe organizations typically focus on external security threats, assuming that staff good will and vendor reliability provide a secure environment.

Today's large-scale data center facilities often serve hundreds or thousands of users who access mainframe batch and timesharing services. System integrity vulnerabilities therefore expose critical company data and resources to internal hacking attempts that may violate regulatory compliance policies, compromise critical information, or cause significant financial losses. Discovering and resolving vulnerabilities helps ensure compliance with corporate governance and standards requirements.

> Without assured system integrity, promised attributes such as security, reliability, and privacy are meaningless.

Until integrity issues are reported, however, they're subject to discovery, malicious exploitation, and accidental encounters. In addition, configuration choices and added system software layers from IBM, ISVs, and local developers can introduce risks not present in z/OS itself.

A powerful z/OS tool, the authorized program facility (APF), lets installations identify system or user programs allowed to use sensitive system functions. To maintain system security and integrity, a program must be authorized by the APF before it can access restricted functions, such as supervisor calls (SVC) or SVC paths.

Authorized programs can do virtually anything; they are essentially operating system extensions. They can enter supervisor state or a system key, modify system control blocks, execute privileged instructions (while in supervisor state), and even turn off logging to cover tracks.

APF helps avoid integrity exposures, just one of which seriously compromises any installation security controls; installations identify libraries containing special functions or programs, called APF libraries. So, clearly, this authorization must be used sparingly and monitored carefully.

In fact, though IBM publication z/OS V1R12.0 MVS Authorized Assembler

Services Guide (SA2207608-15) states:

"It is the responsibility of the installation to verify that any authorized programs added to the system control program will not introduce any integrity exposures," IBM does not provide tools for doing this.

Because of immense and always-increasing mainframe complexity, it's too risky to rely on manual observation of normal system usage to expose such vulnerabilities. So regularly and systematically verifying integrity of full software stacks is essential.

In addition to preserving and verifying system integrity, z/OS system parameters must specify appropriate security. Complete specifications are detailed in the US Defense Information Systems Agency (DISA) Security Technical Implementation Guidelines (STIGs), available at URL iase.disa.mil/stigs/stig/index.html. Separate guidelines cover External Security Managers (ESMs) such as IBM's RACF® and CA Technologies' ACF2® and Top Secret®. A STIGS tool audits hardware configurations, IPL parameters, and security implementations but does not detect integrity exposures.

Being military guidelines, they do not apply to all installations and situations. But they cover generally applicable parameters and configuration controls. Their complexity, however, makes comprehension and compliance challenging.

Finally, corporate IT environments are subject to change, sometimes on a too-hurried basis: tactical or strategic issues can motivate ESM migrations or mergers. The former can be driven by dissatisfaction with function, service, or pricing. The latter occurs with system consolidations, downsizing, acquisitions, etc.

Enter Key Resources, Inc. (KRI)

Key Resources' Vulnerability Analysis Tool (VAT) is an innovative z/OS integrity penetration testing system.

An ethical tool, VAT probes z/OS environments for vulnerabilities, automatically collecting data for IBM, independent software vendors (ISVs), and local development teams.

Operating independently of whichever ESM is in use, VAT assures that system integrity exploits cannot bypass these systems' security protections.

And, of course, VAT identifies z/OS Statement of Integrity violations.

KRI and VAT . . .

- Support latest IBM z/OS Releases;
- Provide comprehensive system hardening assessments for complete mainframe environments, no matter how complex, including z/OS, TSO, VTAM®, JESx, CICS®, USS, TCP/IP, DB2®, etc.;
- Ensure standards compliance via vulnerability, penetration, and malicious user testing;
- Supplement DISA STIGs tool by detecting integrity exposures;
- Use sophisticated tools to perform controlled extracts and generate test cases, shortening review cycles;
- Automate actively probing for vulnerabilities;
- Monitor possible internal security breaches;
- Provide vendors or internal staff actionable reports on integrity exposures, including Supervisor Call (SVC) interfaces, system exits, Program Call (PC) routines, linkage index (LX) interfaces, and Authorized Program Function (APF) programs;
- Assist with ISV product problem management and alerting;
- Focus exclusively on SoI violations, not overlapping with software inventory or patch management tools, which do not find vulnerabilities;
- Is typically run onsite by KRI for first use, then is normally used by installation personnel as part of routine system maintenance; and
- Can be licensed for self-assessment.

KRI Client Advocacy

KRI is an advocate for its clients, recognizing that SoI violations potentially allow bypassing installation security controls, suppressing audit trails, and changing or disclosing mainframe data — no matter which ESM is installed. Understanding the devastating potential of such risks, KRI eliminates them from client systems, since there can be no system security without operating system integrity.

Naturally, ISVs are occasionally unenthusiastic about security problem reports. But KRI's convincingly demonstrating that their software violates the SoI simplifies remediation with clear and concise problem data. ISVs generally accept and act on VAT reports; if necessary, KRI creates security exploits as proof-of-concept for exposures. KRI then verifies that fixes are complete and correct, and do not require special — and error-prone — administrative procedures. Fortunately, IBM and CA are pleased to accept integrity issues found and remediate them.

Vulnerabilities located by VAT violate IBM's Statement of Integrity; they're not speculative or hypothetical problems, and IBM takes them seriously.

Key Resources, Inc. — Small Company Providing High Value

Ray Overby founded KRI, a privately held mainframe IT consulting company with clients in all sectors of business and government, in 1988. Business began with one small contract providing a mainframe security audit to a government agency. Over time, KRI acquired ongoing contracts with some of the largest mainframe-centric corporations in the world.

Overby notes that many years ago, when people thought mainframes were going away, he saw training shift from the mainframe to distributed systems. Now, he says:

> "This shortage of experienced mainframe professionals who are versed in all of the complexities of the System z® mainframe operating environment, combined with the continuous pressures to keep data sources secure, weighs more heavily than ever on corporate and IT security executives."

To fill this gap, while still providing systems programming and development services, KRI evolved to focus on ethical hacking, security audits, and security product conversions using its powerful proprietary sophisticated tools.

KRI tools and services also migrate security databases between ESMs, including preliminary advice, project planning, project management, conversion/merge, and technical programming; and merge security databases from two or more security packages.

Overby wrote about verifying mainframe security in independent magazine z/Journal, "Is Your z/OS System Secure?", available at www.main framezone.com/it-management/is-your-z-os-system-secure.

uPDT Acquisition and Installation

While KRI's services and tools target enterprise-class systems, KRI uses a much smaller — but no less powerful — system for research and development, namely uPDT (Ultimate Personal Development Tool) from Virginia-based Information Technology Company (ITC).

> The uPDt provides a realistic full-function z/OS environment.

In fact, KRI also uses the uPDT for identifying and resolving z/OS problems before they're found on customer systems. Even problem fixes specific to unique client software suites can be developed and validated on the uPDT.

Overby calls the uPDT a very good product, noting, "It has good support; it has been a very good experience for us and I would recommend it to others." He compliments ITC staff as being very knowledgeable technically and appreciates sales/marketing officials accommodating KRI regarding the system's lease.

Small-company KRI offers larger-than-life services and value, ensuring that real-world production systems achieve the promise of IBM's Statement of Integrity. They rely on their development/production platform, ITC's similarly small-system/high-value uPDT.

ITC UltimatePDT (uPDT) Solution

The uPDT technology solution s a complete and ready-to-use mainframe application development system for IBM Independent Software Vendors (ISVs). uPDT systems offer a robust, reliable, and attractively priced platform for IBM System z® mainframe development.

uPDT incorporates the IBM System z Personal Development Tool (zPDT™) with state-of-the-art Intel® 64bit IBM and Lenovo® systems to work seamlessly with the Linux® operating system and IBM System z software. The result is a low-cost, integrated, fully capable mainframe computing system well-suited for development or demonstration purposes.

The zPDT software-based application tool provides an affordable application development and demonstration platform for commercially available System z products. The zPDT enables a virtual System z architecture environment to run in full capacity on Intel platforms — such as a Lenovo laptop or IBM System.

This powerful tool provides:

- Low-cost IBM System z platform for ISV application development and testing
- Portable System z platform for operating system, application and product training, education and demonstration
- Support for developers in remote or multiple locations where personal systems are more efficient and cost effective than dedicating larger server resources
- Freedom from dedicated LPARs on existing systems
- Complete control of a complete System z environment without risk to – or impact on – other people or other development/test/production work

Three zPDT configurations accommodate differing requirements, providing

one, two, or three virtual engines, which can be enabled as separate uniprocessors or as a multiprocessor configuration. Virtual engines can be defined as System z general purpose processors, System z Integrated Information Processors (zIIPs), System z Application Assist Processors (zAAPs), or System z Integrated Facilities for Linux (IFLs).

ITC extends zPDT value and flexibility by creating an underlying image meeting demanding System z development requirements for reliability.

ITC's extensive uPDT design/build/test R&D provides essential experience in configuring systems, providing deployment-ready uPDT systems for productive application development use.

ITC's uPDT system includes a customer-specified hardware platform (laptop, desktop, or server), IBM zPDT technology (USB Hardware key and appropriate 1090 device software), Intel-based Linux (Red Hat® or openSUSE), and selected System z operating systems (z/OS, z/VM®, z/VSE®, Linux on System z). The ITC uPDT is a complete, ready-to-use system, built to unique customer specifications, fully tested, and burned in. ITC also provides first- and second-level uPDT technical support.

Recognizing uPDT systems' mission-critical nature, ITC provides a backup-and-restore facility featuring speed, ease of use, flexibility, and completeness. Menu-driven, it works seamlessly to back up and restore the Linux/zPDT environment and mainframe emulated 3390 volumes.

Information Technology Company, LLC

Since formation in 1992, Information Technology Company, LLC (ITC) has solved clients' real-world IT issues with high-quality service and sound technology. Extensive research, detailed understanding of customer environments, and ongoing R&D efforts —creating value in innovative alternatives for customers— enable ITC to deliver the right solution on time and on budget.

ITC addresses common IT management concerns (e.g., lack of internal financial and human resources for existing operations or undertaking new projects) by providing expertise and experience in all aspects of modern technology. Expertise spans System z mainframes, large scale servers, personal computers, wireless devices, and operating systems and applications working with these platforms.

> ITC solves clients' real-world IT issues with high-quality service and sound technology.

ITC engineers and business staff apply extensive problem-solving knowledge to provide the most efficient and cost-saving solutions. Company projects are not quick-fix shortcuts; managed services are guaranteed for successful completion. This simple philosophy of responsibility and accountability brings a new level of customer care to all projects without surprises or disappointments.

ITC services encompass diverse data center tasks covering every aspect of IT business operation:

- Requirements, analysis and specifications development
- Data center pre-installation preparation
- Hardware and software acquisition planning
- Performance analysis
- Computer system integration with enterprise infrastructure
- Data center procedures development
- Operation, administration and support training
- Remote operation control and monitoring
- Hardware installation and configuration
- Software installation, configuration and customization
- System hardware and software technical support
- Project management
- Disaster recovery design and planning
- Data center relocation

For more information about Key Resources, Inc.: visit www.kr-inc.com

Information Technology Company

Turn your legacy into a legend.™

7389 Lee Highway Suite 210
Falls Church VA 22042
800-994-9441 Fax 703-237-0223
www.p390.com

uPDT information:
www.p390.com/updt.htm