# IBM System z Security
Covers the Enterprise End to End

Analyst: Anne MacFarland

Management Summary

Today's enterprise is not an island, and cannot, by its nature, be a fortress. More information must be shared with a changing litany of business partners and associates, each with varying levels of trust-worthiness. Often, today's business does not control all the assets used in its processes. The binary *yes/no* of data access authorization has been replaced by a need for more granular permissions. With Web Services and SOA, this permission granularity now applies equally to applications and processes. The old controls of perimeters, firewalls, access lists, and anti-virus software are insufficient. Today's business process often is a litany of hops from some end user across the Internet into the depths of your data center – for the purpose of engaging with your core business processes. **As a result, the scope of IT security is expanding, and the focus is changing.**[1]

The increasing breadth of business processes and the consequent spread of business data pose new challenges to IT security. (See Exhibit 1, at the left.). The implacability of audit requires that the new demands outlined above be addressed, it cannot be avoided.
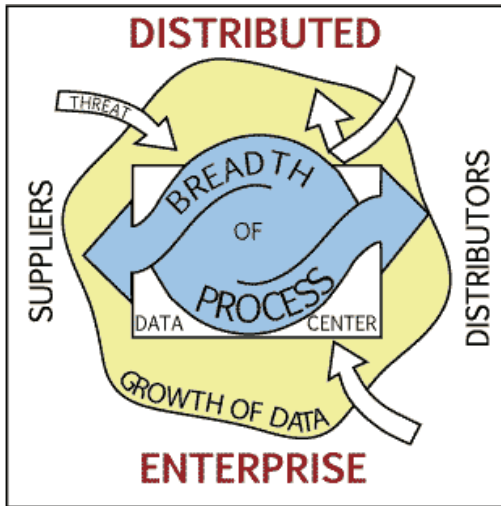
Exhibit 1

Consider the continuing breaches of customer information. Your customer details can be exposed because your business processes aren't confined within the glass walls of your data center. Your sales force and partners want information and process capability available at a click – wherever they are. Self-service by partners and customers satisfies the pace of today's impatient business practices, reduces errors (in many cases), and wrings costs out of doing business. **Increased data use is a win-win-win – except that security may not be baked into all your processes at all locations – and, now, increasing regulations require reporting of breaches and other security lapses.**

For more than four decades, IBM's mainframe has run big business' core processes – in part because of the wealth of controls built into the hardware, operating systems, containers, middleware, and management. Over the years, the benefits of this controlled environment were extended to new workloads in partitions, virtual machines, and in those attached via Web Services. Throughout these developments, security and control systems were evolved to meet new demands. For more details about mainframe security today on IBM's *System z* and how it can benefit your whole enterprise, read on.

---

[1] For a tutorial on the new challenges of enterprise security, see the issue of **Clipper Notes** entitled *The Challenge of Enterprise Security*, dated April 5, 2007, and available at http:www.clipper.com/Research/TCG2007050.pdf.

System z's Domains of Control

IT security must focus on the control of *processes, data,* and *network*, as well as on physical assets and external threats. It must do this - without constraining the business. Being security-rich by design (see Exhibit 2, at the right), *System z* offers a wide range of inherent controls across those domains, as well as explicit security features that promote the security of all enterprise uses of System z.

Process Controls

The IBM mainframe was born with a multi-programming architecture. It sees an application as a system user with an identity and specific rights to specified system assets. System z LPARs (isolated logical partitions), z/OS, and *z/VM* containers meet *EAL5, EAL4+,* and *EAL3* standards, respectively.[2] You can put a z/VM instance inside an LPAR (or inside another z/VM instance, for that matter) to get more degrees of isolation and virtualization. *RACF's*[3] resource management governs and mediates resource use in z/OS, z/VM, and other mainframe environments. IBM's acquisition of Consul adds more usability to existing mainframe controls. (More on Consul later in this bulletin.)

With any application running on z/OS, each resource and data set has an access list of users and groups of users that are allowed to access it. These access lists have a wide range of authorization options that delimits what each user or application can see and do.

Network and Data Controls

Business processes that run on Linux images can be co-located on a System z. There highly-secure logical partitions protect the images. A function called *HiperSockets* can connect them to other images using internal IP communications in system memory. For data that is requested by other applications in the larger enterprise ecosystem, the z/OS TCP/IP stack features integrated intrusion detection capabilities that look for attack patterns.

Encryption

Encryption solutions can protect mainframe data from sniffers and spoofers. Any use of encryption involves the management of security keys. System z's key management and certifi-

---

[2] The Evaluation Assurance Level is an international standard grade of IT element security based on seven levels of test. The highest levels of testing are for elements, like smart cards, that are at particularly high levels of risk.
[3] *Resource Access Control Facility.*

| Exhibit 2 – |
| System z – Security-Rich by Design |

**Exhibit 2 –
System z – Security-Rich by Design**

The IBM mainframe was designed to support business when constrained resources demanded that many applications share compute resources safely. Isolation and control were key system design points because applications had to be isolated from each other. This underlies System z's exceptional systems integrity and contrasts with other platforms that were not designed to prevent conflict.

System z is inherently resistant to hacking and information theft because of the controls built into its hardware microcode to support process isolation and data integrity. Due to the tight integration between the hardware and the z/OS operating system, executable instructions are treated separately, providing additional resistance to buffer overflow attacks. Applications must go through a z/OS control point such as RACF to access resources, and RACF and z/OS can document the request, providing auditing and charge-back capabilities.

RACF, an optional feature of z/OS, manages the security of the environment using all the security control points built into the System z architecture and the z/OS operating environment. All processes are allocated resources, and, while these allocations may be flexible, processes can be limited in their authorities. System z allows other operating systems, including Linux, to run within its secure partitions. They all benefit from the strict civil procedures built into System z.

---

cate authority capabilities allow businesses to use encryption effectively on an enterprise scale.

Network encryption is familiar to many as *SSL* or its successor-standard *TLS (Transport Layer Security)*. Along with *IPsec,* these are frequently used with a Virtual Private Network (VPN) in Internet-based commerce. z/OS supports SSL, TLS, IPSec, OpenSSH, and PGP, plus multiple symmetric and asymmetric encryption methods.

System z's optional *CryptoExpress2* hardware encryption co-processor accelerates the handshakes of SSL/TLS to support a very-high rate of transactions. **Today's *System z9* mainframes have the optional CryptoExpress2 feature that provides tamper-resistant hard-**

ware, which in turn secures a vault of encryption keys. This vault can contain both *secure key* – keys that are only visible in the Crypto-Express2 hardware card – and *clear key* applications, based on configuration options. Crypto-Express2 also offers *CVV* (Card Verification Values) *generation* for credit card processing and *verification services for 19-digit PANs* (Primary Account Number), providing advanced anti-fraud security.

The *Integrated Cryptographic Service Facility* or *ICSF*, a component of z/OS, is a valuable asset in securing and ensuring the integrity of your keys. You can create a key today and store it securely (by encrypting it under your master key), and that same key value can be available 10 or 20 years from now. Even though the external representation of that key might change over time (i.e., with master key changes or key rotation policies), the underlying key is preserved.

The actual exchange of public keys usually is accomplished using digital certificates – the identity authentication "notary public" of the Internet. **The PKI Services component of z/OS provides an attractive alternative to the added expense of third-party digital certificate hosting. It allows z/OS customers to become their own Certificate Authority, reducing additional costs.** This is particularly valuable to establishments that need to secure access to hundreds or thousands of remote servers and devices. For an enterprise that needs, for example, to authenticate the end points of a VPN connection between data centers and branch offices and remote workers, **System z can be the sole Certificate Authority for all of your enterprise's technology platforms.**

Unencrypted tapes have become a conspicuous example of what not to do for sharing potentially sensitive data with business partners. z/OS has a flexible, server-based encryption product (*Encryption Facility for z/OS*) with flexible options for exchanging encrypted data on tape. In addition, IBM recently announced the IBM *TS1120*, a tape drive that encrypts at close to line speed.[4] This lets tape encryption become a routine part of data management as opposed to a separately-invoked function. For those who use tape, and particularly for those who ship tapes,

this is a sensible way to support these operations. In both tape solutions, you can secure the access to these tapes by managing and distributing public keys and securely hosting private keys using the mainframe's key management technologies.

IP Sec

As businesses grow more distributed, develop more "lights-out" IT environments at the edge of the enterprise, and extend business processes across more networks including the Internet, **full security dictates that encryption should cover endpoint to endpoint, not merely endpoint to a network switch.** System z supports true end-to-end encryption, even to a laptop[5] or a printer,[6] with IPSec. This removes the connection to the switch as a point of compromise for particularly sensitive transmissions and supports compliance in regulated industries. z/OS implements IPSec within the secure environment of System z, removing another risk exposure.

Additionally, in z/OS 1.8, offloading IPSec to a specialty *zIIP*[7] processor accelerates processing in the same way System z offloads Java execution to one of its *zAAP* specialty processors. This improves the price/performance of end-to-end encryption.

With the inherent process, data, and network controls described above, and the addition of a *WebSphere* portal, business processes can be tracked from core to its final delivery to an end user. The integration of audit logs used by *Consul InSight* (more below) makes possible a process audit across mainframe, *UNIX*, and *Windows* environments. This allows the full breadth of participants to be part of a unified enterprise security strategy.

System z's Role in Enterprise IT Security

Security is an ever-evolving trade-off between opportunity and risk. Recent business focus has been on expanding opportunity, but mitigating risk must not lag far behind. *Assessment*, *controlling access*, *monitoring*, and *defending* are the four corners of any security initiative. The first step in risk mitigation is

---

[4] For more information about the TS 1120, see **The Clipper Group Navigator** entitled *IBM Gives Enterprise Options for Encryption*, dated August 28, 2006, and available at http://www.clipper.com/research/TCG2006077.pdf.

[5] With the Java decryption client mentioned above.

[6] With the IBM *InfoPrinters*.

[7] Note that the LPARs and z/VMs that contain System z applications can include access to System z specialty engines.

Exhibit 3 – Further Insight into Enterprise Security

In *The Challenge of Enterprise Security**, Clipper's Managing Director Mike Kahn concludes that "*managing* and *protecting* applications, data, and users in today's enterprise environment are each complex tasks. Since each goes hand in hand with the others, the overall challenge is formidable." He added: "While we may want to specify security requirements for groups of users, classes of data, and applied uses (applications) individually, it is the interrelationship among all three for which security needs to be implemented, in an auditable manner." This challenge exists independent of the server architecture and platforms.

He went on to explain the generic requirements: "What we now require is an IT environment where we can secure work in isolation and in relation to other work and systems processes, in an auditable manner." Key to achieving this is "transparency" to all people, processes, applications, administrators, assets, etc., who are not permitted to see or use these objects. Equally important is the record keeping of use and access to all resources and objects, creating and protecting a secure audit trail. This is important, because (1) "Your greatest threats are inside your enterprise"; and (2) "You may be changing your business models and underlying IT requirements in many significant ways."

He further explained: "If your systems cannot secure the applications and data adequately (to a level of enough detail to achieve your objectives) then your hoped-for success ends here. If you cannot manage all of your resources (and ultimately the applications and user experiences) to predefined service levels, through Service Level Agreements (SLAs) or other means, then you may be secure but not getting the job done. Once you accept the concept of the big picture of security requirements, you must append these to your operational business requirements. To have security but not meet needed levels of service or to meet the needed levels of services without adequate security and auditability just isn't good enough. You've got to do them both and do them well, i.e., *serve* applications and data and *protect* them, the users, and your infrastructure." That is your challenge.

---

*See footnote on page 1 for reference to this issue of Clipper Notes.

---

assessment.[8] However, security controls also must cover the "four corners."

- *Assessment* is important because security only works if the entire domain of concern is covered with consistent policies.
- *Access Control* is key because inappropriate access is a source of most risks. In enterprise environments, the federating of identity, authentication, and access management is key to keeping the whole business secure in an unobtrusive way.
- *Monitoring* is required even with proper assessment and access controls because breaches – some unintentional and some not – can and do happen with authorized users, and new threats will crop up as business processes evolve.
- *Defending* deals with the many risks that cannot be avoided by adding safeguards such as encryption and intrusion prevention services

to mitigate risk. These safeguards must be supported in a way that makes the *who*, *what*, *where*, and *when* of auditing easy, not just for regulatory reasons but also to assure the health and survival of the business. (See Exhibit 3, above, for a further discussion on the challenges of enterprise security.)

Assessment

The overall environment that must be assessed grows larger as processes transcend platforms, geographies, and organizational affiliations. The need to document exactly *who did what*, for corporate governance or regulatory compliance, adds to the granularity of the assessment. **You must determine where security is needed, but this can be achieved by applying a high level of security to all components and then relaxing some constraints where needed and appropriate.**[9] There are some environments in which the documentation of what has happened is enough (say, the behavior of website visitors). In other cases, the access documentation (logs, for instance) also must be

---

[8] Decades of data center experience have taught us that assessment can be a very broad and difficult challenge in the larger, ever-changing enterprise. In fact, usually it is easier to protect everything under one set of common but broad security policies and then to lessen this protection on specific applications, resources, objects, etc., when an exception is justified by business requirement or specific mandate.

[9] See a relevant discussion in the issue of Clipper Notes cited in Footnote #1.

secured to assure their completeness and integrity. However, in many cases, more is needed to protect the organization. It is important to assess *where* you will run your security and *how* you secure the security process. **One sensible answer is to tie your security in with your most inherently secure platform – System z.**

Access Control

In order to support compliance requirements across the enterprise, identity authentication and access management is required and must be coordinated among segregated parts. Many IBM and third-party software products enhance security on the mainframe and on systems that connect to System z.[10] IBM's *Tivoli Identity Manager*, *Tivoli Access Manager*, and *Tivoli Federated Identity Manager* provide an edge-to-edge coherence for identity and access management, working with RACF for z/OS. These products meet all of the security standards that are being ratified in this area. They integrate identity and access management across mainframes and distributed applications, and add security to Web Services environments.

Now with Tivoli Identity Manager on System z, rich identity management features provide a highly-secure, highly-available, scalable identity solution. On z/OS, Tivoli Federated Identity Manager provides security integration for web services that use z/OS CICS or other z/OS subsystems, using z/OS security services. Remember, **facilitating federated identity without securing the federating process is just opening up another seam of risk in your operations.** Consider the benefits of placing your federating options on System z.

With z/OS 1.8, System z gains additional LDAP support via the *IBM Tivoli Directory Server* for z/OS, which implements an LDAP server that takes advantage of the capabilities of z/OS and System z to scale and meet the needs of an enterprise wide directory. This server plays a dual role. First, it serves as a capable enterprise-wide directory. Second, it enables controlled access to RACF's security data and security primitives (such as authentication and access control) and audit functions (which

enable other applications and platforms to use RACF's security capabilities in a controlled fashion).

Defending

As discussed, System z has layers of defense protecting the processes and data that are hosted by the mainframe**.** System z's encryption offers a wealth of options to protect data both at rest and in flight. Application hosting environments that run on the System z platform, like DB2 for z/OS or WebSphere for z/OS, have additional controls. **System z also supports enterprise-wide defensive strategies.**

Whether using System z LPARs or a z/VM guest containing a Linux image to compartmentalize and isolate processes, System z is a great location for a Web-facing demilitarized zone (DMZ). On other platforms, this may be a dangerous concept. With System z's isolation, it is prudent – and very useful. Think of collapsing your firewall and Web tier to run in partitions or z/VMs on System z, close to the core databases that support your business. Further protection can be provided with the *Intrusion Detection Services* on z/OS. Such a move could help make all the business processes that leverage the Internet more efficient and more secure.[11]

Monitoring

System z has always had a comprehensive sense of what was going on within its borders through the auditing capabilities of RACF. With Consul, z/OS gets many capabilities that make this security information more broadly useful and actionable.

The *Consul zSecure Suite* adds a user-friendly layer onto mainframe service logs that enable superior administration coupled with audit, alert, and monitoring capabilities for RACF.

- *zLock* uses rules to verify commands to make sure that security policies are enforced. It increases the security of your RACF mainframe environment further by taking more control of administrative actions. It enforces limits on what systems administrators can do.

- *zAudit* works with RACF to produce an audit trail of a resource or a user. With zAudit, audit becomes a part of normal routine not an

---

[10] For example, Stonesoft's *StoneGate* provides application firewalls – the next step after network firewalls – for the System z environment. It is typical of the many products that software vendors have developed and enhanced over the years to add more security to distributed operations involving the mainframe. The inherent integrity and availability of the platform makes it a great place from which to stage security operations.

[11] This illustrates how application workloads can benefit from co-location with z/OS on a System z. The z/OS control systems can manage the new workload containers and flexibly allocate resources to them, as needed. The result is a flexible yet secure environment for key business functions.

exceptional event. It identifies not only who is doing what but also what is out of the ordinary.

- *zAdmin*, *zVisual*, and *zToolkit* make RACF administration easier and more efficient. zVisual shows RACF information in a user-friendly context, so the administrators can be more effective, less error-prone, and can drill down to the details if need be. More significantly, it allows security functions to be delegated and segregated by dashboard capabilities, permitting the *separation of duties* that underlies the integrity of the security process.

- *Consul InSight* translates logs from different systems into a business-facing compliance dashboard that can track processes in their hops across the enterprise and can alert on business policy exceptions.[12]

Moving Forward

The mainframe places security as one of its highest priorities, in terms of both product evolution and testing. It has extended its security benefits to other platforms that are the tenants of its containers and to the processes that transcend its borders. Its key storage and management capabilities, identity management, directory capabilities, and certificate authority solutions, are assets that can be leveraged by the larger environment in which it sits.

Mainframe applications have been evolving to meet new security challenges and new computing architectures. *CICS*[13] has been accessible via Web Services for years, and now has been tooled to participate fully in service-oriented environments (SOAs). DB2 can now store XML natively (not just as blobs) – something that is very helpful in the administration of SOA environments. Because of their heritage, experienced mainframe folks understand what is needed to secure multi-tenancy *and* multiple computing processes. This is new learning for many IT professionals who have experience

only with other platforms.

Conclusion

To be *efficient*, computing must be inherently secure. Otherwise, greater efficiencies just increase the velocity of security threats to the point where aggregated security becomes unmanageable. To be *effective*, security must match the scope of enterprise business processes, yet not impair process efficiency. This is a matter of bringing the ACID[14] characteristics of IT transactions to IT architecture and thinking – and leveraging them to secure the enterprise. What is needed is an integrated security solution – with the ability to spread, where needed – to secure business processes and business information; this is an attractive and much saner proposition.

The mainframe has been working in this mode and meeting such challenges for a long time. System z offers well-honed and time-tested capabilities that help you achieve security, corporate governance, and regulatory compliance without changing how you do business. **The breadth of its security and the granularity of its control systems may be another good reason to rethink** *what you do, where*, **and** *how* **System z should play in ensuring your enterprise's security.**

Bottom Line:

The more the mainframe secures, the better the security across the enterprise.

SM

---

[12] Consul can access logs from System z, Windows, Linux, and UNIX. It can access application logs from SAP, Oracle, Microsoft *SQL Server*, and *UDB*. It has plug-ins to support reporting for HIPAA, SOX, ISO 17799, GLBA, and BASEL2. *InSight* also supports a real-time dashboard for *zAudit's* tracking of the use of special privileges, in order to recognize and prevent misuse. For those with less need for real-time updates, Consul information can be delivered via XML as a Web Browser, spreadsheet, or email, or via the ISPF mainframe interface.

[13] CICS stands for Customer Information Control Systems. It underlies the functionality of bank tellers and point-of-sale systems across the globe.

[14] ACID stands for Atomic, Consistent, Isolated, and Durable.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

➢ *The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.*

About the Author

Anne MacFarland is Director of Data Strategies and Information Solutions for The Clipper Group. Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

➢ *Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)*

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, **Clipper Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.