PKWARE®

Spotlight on Mainframe Security: Privacy in the Data Center

PKWARE WHITE PAPER

Table of Contents

Spotlight on Mainframe Security: Privacy in the Data Center

In the past, data center security was simpler to implement; in fact, there was a time when data center managers could see all the inputs and outputs to the mainframe in one or two rooms. However, this was when data was input via punched cards and output was recorded on tape or impact printers using green bar paper. A terminal had to be added as a logical unit and data center managers knew exactly who had access to the mainframe. Even when someone was logged in, managers always knew exactly what users were doing. Because computing resources were so precious, any abnormal behavior would have some effect on the environment. The SNA network was secured because all the devices on the network were defined. A physical survey of the data center was all that was needed to ensure it was secured.

New technology and constant market pressures have caused simple data center security to be a thing of the past. Today's market requires constant improvements in worker productivity. The advent of personal computing, Local Area Networks (LANs), and the Internet have led to a time of "pervasive connectedness," even for the mainframe Moreover, the market bias has moved from allowing only the "select few" to access information to a stance of "information for all," something original mainframe design and scope never contemplated.

Today, in some ways, the mainframe is no different from any UNIX or Windows server. It is TCP/IP connected and serves the data needs of almost every endpoint on the network. Just because the mainframe still resides in the glass house does not mean that it is as safe as it was 25 years ago; the mainframe sitting on the stark white raised floor of the data center is no longer the "air gapped" icon of data protection.

Equally, the speed with which sensitive data on the mainframe can be converted to cash by cyber crooks has increased – the affects of pervasive connectedness are not limited to encroachments on the legacy mainframe identity and access management schemes. A credit card number stolen from the data center can be sold over the Internet in seconds. According to many, 70% of all mission critical data remains on the mainframe and much of that data relates to customer and consumer information. Yet, contemporary market conditions demand "always-on" access to data in order to support online shopping, administration of retail banking, brokerage or other financial accounts, and other needs. Significant actions with potentially grave repercussions can be performed in a completely faceless manner. The drive to satisfy customer demands for convenience, serving a 24/7 global market place, has given rise to risks previously not looked for that must now be mitigated.

The consequence of increasing customer demands is that the risk to data becomes an issue, not just to the technologists who manage it, but to legislators and industry regulators. Protection of data privacy is now one of the principal areas of focus in each and every technology audit or review; and demonstration that appropriate best practice controls are in place is mandatory to avoid disruptions to technology and business plans.

From Terminal Server to Data Server

The original workload profile of the mainframe was much different than it is today. Dumb terminals with green screens illuminated the office space with CICS panels, green bar reports littered the desks, and there were fewer users that directly interacted with the mainframe. Today, there might not be as many users that directly interact with the mainframe through ISPF or CICS, but the number of users and programs that access information on the mainframe has exploded.

Systems Programmers can now only guess how many external systems they are interfacing with between CICS, WebSphere, MQ, DB2, and other mainframe systems providing the back-end and transaction management backbone of web-form presented applications. To a useful degree, the Security Servers (IBM RACF, CA-Top Secret, and CA-ACF2) have kept up with the exponential growth in the number of TCP/IP connections to the mainframe, but their utility in protecting sensitive information remains limited, providing almost no protection beyond the perimeter of the mainframe. When data from z/OS is transferred to another operating system, it is no longer under the umbrella of protection that the Security Servers can provide. How is that data being protected once it passes from z/OS to another operating system like UNIX, Linux, or Windows? Can you really rely on the access controls for those operating systems to protect the data in the same way, using the same resources and controls as on z/OS?

The mainframe data center initially found itself ill prepared to address the combined risks of increased connectedness and elevated value of sensitive information to the online crook. The industry had been focused on the need for operational excellence, to accomplish more and more work through automation while containing the costs associated with infrastructure and application development. It has not been trivial to add data protection to existing applications and workflows, particularly since some applications have been developed over a generation and represent highly critical and complex sets of business rules (which, unfortunately, are sometimes not well documented outside the code itself). While auditors and

regulators demand that protection of sensitive data increase to mitigate new risks, stakeholders and stockholders still require that operations remain lean to contain costs.

In that context, an obvious response to protect the privacy of data was the use of encryption. Encryption of sensitive data ensures that online crooks cannot make use of stolen data without access to the encryption algorithms and encryption/decryption keys. The question the industry faced then and now is, where and how can encryption be best applied to mitigate the most critical, most broad-reaching risks? Careful thought isolated the options into three general areas: disk encryption, transport encryption, and encryption attached to the data itself.

Disk encryption seems an obvious response – if all the data on all the DASD in the data center is encrypted, then all risk would be mitigated, right? The hesitance of the market to pursue this option stems directly from the issues underlying the approach. Full disk encryption in the hardware is a necessary layer of security that protects customers when an IBM FE, without the need to destroy or wipe the data off the drive, removes a RAID 5 disk from a DS8000 series cabinet. The IBM FE can leave with the drive confident that all the data on the drive itself is encrypted and not accessible by anyone once it leaves the premises. However, when the DS8000 is up and operational, all the data on those encrypted disks are accessible, only protected by the layers of security that Security Server has to offer.

The second encryption approach is transport encryption, wherein data is protected as it leaves one point and is transmitted to a receiving point. This approach is widely accepted, offering the advantage that it can be applied naturally as a new, non-disruptive step in existing workflows. Transport encryption does require that both the sender and the receiver use compatible applications and exchange encryption keys. When in place, it then provides significant mitigation to the risk of data being intercepted and used for dishonest purposes. While widely used, many organizations are finding the transport encryption approach lacking in a couple of specific regards. First, the most common application used for this purpose is provided commercially by a well-known enterprise software product vendor; and many data center managers complain of the licensing expense represented by the annual subscription renewal for the product. Perhaps more important in the contemporary circumstance is that the approach still leaves gaps in data protection in the following instances: when the data is sitting on an intermediate server waiting for transmission; when it is written to physical media; and when it sits within the recipient's data center, on the receiving transmission server or on physical media.

Data-centric Security

The gap between the need for security and risk remediations applied, remained so broad for such a period The third approach mentioned is encryption attached to the data itself. When such data–centric encryption is put to use in your data center operations, it offers another layer of protection to your data. A data-centric security approach encrypts the data so that whether the data remains on z/OS or moves to another platform, the data itself is protected and can only be decrypted by the authorized users or systems with access to the private keys that allow them to decrypt the data. This provides a way to protect the data itself, without having to rely on the access control mechanisms on various different operating systems and platforms.

Data centers increasingly rely on a layered security approach, as no one layer of protection is enough when it comes to information security. Given the pervasive connectivity of z/OS with TCP/IP, data-centric security provides a means for another layer of security on the platform. Even if the data you are protecting is never intended to leave z/OS, it still remains protected at rest and in motion, should things change and

the data needs to be shared with others.

Considering the Data-centric Security Approach

Data-centric security does not require you to rebuild all your z/OS applications to accommodate encryption, as it is typically integrated incrementally into existing online and batch environments. File-based encryption can occur by augmenting existing batch and online environments so that you decrypt information needed by applications just-in-time, and encrypt the information when the originating applications complete (or even before – emerging best practices look to have data protected record-by-record as it is produced by applications or extracted from the database). This does not require any changes to existing application programs and still protects your information at rest.

Because file encryption/decryption can be performed at the point of file creation and use, the operations are more parallelized, thus foregoing wholesale changes into the existing batch schedules. It also means that only the sensitive data is being protected, as opposed to a rote approach of encrypting all data. Even better, System z processors that you have already purchased come ready with hardware cryptographic capabilities such as CPACF (CP Assist for Cryptographic Functions) which also lessens the impact of securing sensitive files in existing operations, as CPACF can greatly accelerate cryptographic calculations when compared to software equivalents.

Data-in-Motion

Because z/OS continues to be the hub and host of enterprise data, feeding all enterprise applications on all platforms, data must be transported off of z/OS. Many times this involves an intermediate server that is used for transport and rendezvous with the off-frame applications. While the transport from z/OS to the UNIX/Linux/Windows server might be secured through Secure FTP or other means, it is no longer under the same protection as it was on z/OS, introducing vulnerability and exposure. As mainframe data travels outside of existing organizational access controls and transport encryption, it will eventually reside outside the originating data center protections and policies. Data exchange outside the organization typically results in the use of even more intermediate servers, on which unencrypted data is more vulnerable as access controls can vary wildly across platforms. Relying only on encrypting the transport device for data as it leaves the organization is simply not enough to fully protect sensitive information. Using data-centric security to encrypt the information on z/OS before it leaves the organization is an imperative best practice.

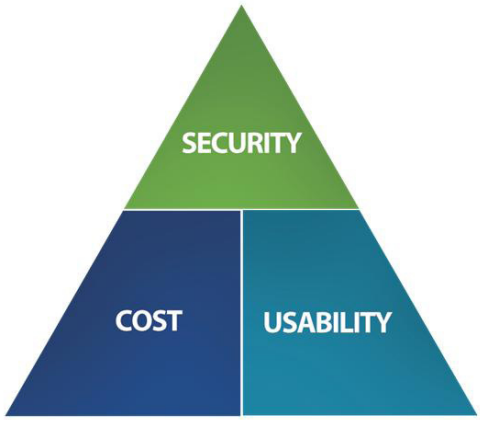
If the data is secured through data-centric encryption on z/OS before it is transported, then it is secure in transmission and remains secure when it lands on the intermediate server and beyond. This granular layer of protection allows sensitive data to travel safely as the security travels with it. Just like in the data-at-rest scenario, the information only needs to be decrypted when it is needed by the downstream application. This approach offers additional opportunities for managing expenses; once the data is protected directly with data-centric encryption, it can be sent by the least expensive means appropriate - even unprotected, shared networks - without placing the protected data at risk. Moreover, common off-the-shelf applications currently available to the market allow organizations to standardize on a single encryption approach that is cost-effective for an organization to acquire. They then make the necessary complementary application available to partners at no acquisition cost to them, side-stepping some of the objections leveled at transport encryption.

SOA and Mainframe Modernization Data Privacy

Organizations that see z/OS as the cornerstone of data management are looking for ways to leverage their existing investment and extend the reach of z/OS in their organization. SOA (Service Oriented Archi-

tecture) and mainframe modernization strive to make data easy to use and inexpensive to access. These trends, while necessary, only expand the risks to which mainframe data is exposed. This raises a conundrum because security can't be ignored, but at the same time it must be easy to use and cost-effective to implement and access.

The security triangle shown below, analogous to the well-known project management triangle, illustrates what systems and application architects must deal with on a daily basis. The constraints in the security triangle are listed as "Security," "Usability," and "Cost," where each side represents a constraint. In addition, one side of the triangle cannot be changed without affecting the others. The usability constraint refers to how usable the security will be once implemented. The cost constraint refers to the amount of money available for the task; and the security constraint points to how secure the task's end result will be. These three constraints are often competing - increased security typically means decreased usability and increased costs, increased usability constraint could mean increased costs and reduced security, and a slashed budget could mean decreased usability and security. Data-centric security helps to ease the impacts of the competing constraints in a SOA environment as it allows the security to be effective across platforms and implemented incrementally.



Conclusion

The mainframe is a vital and, by many accounts, growing resource for managing an organization's mission-critical applications and data. Even in that light, however, the challenges and opportunities faced by the mainframe have evolved since its original inception, leading to new compliance expectations. Protecting the privacy of sensitive mainframe data is paramount among new compliance requirements; and encryption is the natural means to achieve this privacy. Of the common encryption approaches available, disk encryption does not address many critical needs and transport encryption leaves gaps in protection even while being frequently used. Data-centric encryption offers the best combination of operational efficiency, reduced costs, and broad risk mitigation.

About the Authors

Joe Sturonas, Chief Technology Officer, PKWARE, Inc.
Joe Sturonas was previously CTO of Premonition Software, as well as Spirian Technologies. He was also a founding member of OneNetPlus.com, an Internet-centric Management Service Provider. Mr. Sturonas holds a MS degree in Computer Science from DePaul University.

Jeff Cherrington, Vice President of Product Management, PKWARE, Inc.
Jeff Cherrington was previously Vice President at Bank One, Director of Product Management & Consulting Services for WorkPoint, Inc., and has also worked with other top U.S. and international financial services

companies. Mr. Cherrington has an Executive MBA degree from the University of Nebraska.

About PKWARE, Inc.

As the inventor and continuing innovator of the ZIP standard, PKWARE, Inc. is a global technology leader known around the world as the expert in data compression and file management. With the launch of SecureZIP in 2005, PKWARE successfully entered the data security marketplace, combining ZIP compression and strong encryption to deliver a data-centric security solution. Today, SecureZIP and PKZIP are used by over 200 government agencies and 30,000 corporate entities, including 90% of the Fortune 100. Organizations in financial services, banking, government, healthcare, and retail use PKWARE solutions daily to protect sensitive data, meet compliance requirements, avoid liability risk, and reduce their overall costs and operational overhead. PKWARE, a privately held company, was founded in 1986 and is based in Milwaukee, Wisconsin; additional offices are located in New York, Ohio and the United Kingdom.

United States
648 N. Plankinton Ave., Suite 220
Milwaukee, WI 53203
1.888.4.PKWARE
www.pkware.com

UK/EMEA
Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom

PKWARE®