How Secure is Your Data?

By Rick Rudd
IBM Systems and Technology Group

Executive Overview

Newspapers, television and trade publications are full of stories covering breaches in corporate security and the resultant exposure of proprietary business data and confidential customer information. Missing files from secure government offices, the theft of consumer records, the invasion of private medical records and significant data losses are becoming almost commonplace. Security experts identified about 79 million identity exposures in 2007, four times as many exposures as were recorded in 2006. When they become available, the results for 2008 are expected to show even further increases over what we saw in 2007.

In its 2007 annual study, sponsored by PGP Corporation, the Ponemon Institute, a privacy and information management research firm, said that the average cost to US companies of a single data breach incident was more than $6.3 million. For companies based in the United Kingdom, the financial exposure was £1.4 million on average.

For some unscrupulous individuals, there's a fortune to be made in the misuse of sensitive data, whether it's acquired through an unsecured network, a calculated software attack on a company's computer systems, or the theft of an individual server or disk drive. Sensitive data can even be exposed inadvertently when a server or drive is returned for service, or when someone improperly discards a drive.

Due to the increasing business risk associated with data breaches, companies are deploying data security solutions at an ever-increasing rate. Another factor driving increased deployment of more secure computing systems is that security and data protection regulations mandate that organizations protect data to a certain standard, often leaving them no choice but to better protect their data using the newest and most secure technologies available. Such regulations may be governmental in nature or industry-specific, such as healthcare, finance, or retail. Enterprises are struggling to comply with the applicable regulations within the framework of a limited IT budget. From a business perspective, the risk of non-compliance may be an even greater exposure than the threat of an actual data breach.

This paper describes some of the hardware and firmware security features that make the new generation of IBM® System x® and BladeCenter® servers more secure than ever—protecting you, your business and your customers.

Server Technology that Protects Your Data

A new generation of IBM servers with the new Intel® Xeon® 5500 Series processors helps protect customers against data breaches from network, software and physical attacks. They utilize integral security features including hardware and firmware protect the systems and software. The ultimate goal of these innovative designs is to maintain the security and integrity of the data these systems contain.

Beginning with the IBM **System x3550 M2** and **x3650 M2** rack servers, **BladeCenter HS22** blade server, and **System x iDataPlex™ dx360 M2** servers, these new products will help IBM customers protect their data through a variety of technological features, primarily in four major categories:

- The systems employ the trusted computing architecture as defined by the Trusted Computing Group (TCG) industry consortium. This architecture consists of a hardware-based Trusted Platform Module (TPM) and trusted firmware that work together to provide secure access to the TPM and establishing a verifiably secure environment on these systems.
- Strong, hardware-based drive encryption provides a high level of confidence that a customer's data privacy will be protected under all attack scenarios, with strong protection of security keys, a management interface solution that is easy to navigate and use with no compromise to system or I/O performance.

- Security capabilities that physically ensure the integrity of the server and the valuable information it contains.
- Storage and client virtualization that brings data from disparate servers and client workstations inside the secure walls of the data center

Trusted Computing Platform (TCP)

The Trusted Computing Platform consists of two components: a Trusted Platform Module and trusted firmware.

The Trusted Platform Module

The Trusted Platform Module (TPM) is a hardware-based security and cryptography processor that is integral to the new IBM server platforms, the x3550 M2, x3650 M2, and HS22. It supports a range of capabilities and security solutions, such as protecting stored data, making strong client authentication easier and more affordable, and implementing network access controls to improve overall endpoint security.

The TPM serves as a secure repository for digital certificates, passwords, and other user credentials and important confidential information. It also facilitates key management and escrow for verifying the identity of a system. In addition, it can securely sign, encrypt, and decrypt e-mails and digital documents, provide the second factor in multi-factor authentication, and help assess the security and integrity of the server.

Numerous government agencies, including the US Department of Defense (DoD), explicitly require a TPM for all new computer purchases.

Trusted Firmware

The TPM delivers strong security capabilities, but it is of little use without support in the underlying hardware, firmware and software platforms. The new IBM servers fully enable the TPM to protect the integrity of the IBM firmware, while enabling software applications to take advantage of the security functions the TPM provides. The TPM also enables a system user to securely assert physical presence or to authorize highly sensitive security operations, such as changing the TPM owner or updating the TPM firmware.

What is it that makes these new server platforms so trusted? They implement the Integrity Measurement Architecture as defined by the Trusted Computing Group. At the heart of these systems is the Core Root of Trust for Measurement (CRTM). This is the firmware that is always executed first, every time the server performs a power-on reset. The CRTM:

1. Initializes the TPM and the integrity measurements log
2. Measures the next block of firmware that executes the next step of platform initialization, records the measured value in the log and then updates the TPM with the measured value
3. Passes control to the next (measured) firmware block to execute

The CRTM firmware establishes a secure boot sequence by starting the integrity measurements chain and creating a series of steps of transitive trust that continues through all of the pre-boot firmware components on up to the operating system loader, where it can continue with a secure OS loader and OS kernel or hypervisor.

When combined with the TPM's support for integrity measurements and remote attestation, the CRTM firmware enables establishment of trust in the operating environment and in applications. These capabilities are also leveraged by systems management applications, such as IBM

Systems Director[1], for monitoring and compliance reporting, as well as by technologies like Trusted Network Connect to protect a customer's data and allow the customers to detect, confine and remediate issues, to maintain a secure server environment that is in compliance at all times.

Through a special hardware assist feature, the CRTM firmware is protected from being modified at any time by any other firmware or application running on the system. However, it can still be updated securely with an appropriate firmware update package, provided it is signed by an IBM secure server. The CRTM firmware checks for pending updates each time it executes and then validates and installs any updates required to upgrade itself as necessary. Once there are no longer any CRTM updates pending, the CRTM firmware locks itself down and continues with the trusted boot process as described above. This allows the upgrading of the CRTM firmware itself through a software tool that stores the update packages in a secure staging area and reboots the server to first validate and then apply any pending updates.

Encryption of Stored Data

While a trusted computing platform protects against network and software attacks that attempt to steal data by exploiting software vulnerabilities or installing malicious software to get data out through the network, additional protection is required to safeguard data that is stored on a system's data storage drives. Even the strongest system security cannot prevent unauthorized access to the data on a drive once it is physically removed from the system, which is becoming simpler than ever to do. (A hot-swap 2.5-inch drive can easily be carried away in a shirt-pocket.) Similarly, pocket-sized high-capacity external USB drives make it easy for a thief to copy large quantities of proprietary data.

Encryption of the data on the drive is the premier solution to protect privacy by ensuring that only authorized systems and users can read it. Even physical access to the media does not compromise the privacy of the data as there is no way to decrypt it without the appropriate authorization.

Encryption of stored data protects the privacy of the data across multiple potential data exposure scenarios:

- Hard disk and solid-state drives or entire computers may be stolen, with threats coming from both outsiders and insiders
- When improperly disposed of, drives may later fall into the wrong hands
- Sensitive data on disk drives may be exposed when a system is returned to a vendor for service

To fulfill the requirement for protection of data at rest at all times, IBM offers a hardware-based RAID encryption solution called the **ServeRAID®-MR10is VAULT** adapter. This SAS/SATA RAID storage controller card includes a high-performance, hardware-based storage encryption engine. The ServeRAID-MR10is VAULT is an optional adapter that provides two key functions. First, it operates as a standard RAID adapter card that enables multiple drives to be configured to provide a highly reliable data storage solution. The ServeRAID-MR10is VAULT supports all major RAID levels:

- RAID-0 (striping, optimized for performance and capacity, not availability)
- RAID-1 (mirroring, better availability, lower performance and capacity)
- RAID-10 (striped mirroring, better availability, better performance)
- RAID-5 (striping with parity, great for availability, with reasonable performance)
- RAID-6 (striping with double parity, highest availability, with reasonable performance)

[1] Included at no extra charge with most IBM System x, BladeCenter and iDataPlex servers.

- RAID 50 and RAID 60, which use striping and parity in mirrored arrays to meet a wide variety of availability and performance requirements.

The most compelling feature of this product however, is not its RAID capabilities, but rather its integrated encryption technology, incorporating IEEE-1619 XTS-AES 256 standard disk encryption. With the ServeRAID-MR10is VAULT, if a drive is stolen the data on it is completely inaccessible without the unique encryption key associated with that drive and data. Depending on how the encryption is configured on a given server, the data in that server can still be completely protected even if the entire server is stolen.

Because it is a hardware-based solution, the ServeRAID-MR10is VAULT has two distinct advantages over competitive software-based encryption solutions:

- Encryption software typically stores encryption keys in system memory, which makes it vulnerable to software attacks or simple physical memory attacks. The ServeRAID-MR10is VAULT solution is more secure because the keys are stored by a specialized hardware device and therefore better isolated from attacks from software running on the server.
- Any type of encryption is typically a compute-intensive task. Encryption in software consumes a great deal of computing resources on a server, resources that are no longer available to end user applications. This can significantly degrade the performance of the applications running on the server. The ServeRAID-MR10is VAULT hardware encryption engine offloads the cryptographic processing from the server's main processors, so that server performance is not degraded by the data encryption activities being performed by the adapter.

Later in 2009, the TPM-enabled IBM systems will support **Full Disk Encryption (FDE) drives** in addition to the hardware encryption currently provided by the ServeRAID-MR10is VAULT adapter. These drives will employ an encryption engine in the disk drive itself, providing even greater encryption performance when a large number of drives are attached to a server.

The TPM-enabled IBM systems will also support **Microsoft® Windows® BitLocker** encryption, including the secure boot option that uses the TPM to lock down the pre-boot state of the system by binding the encryption key to it.

Physical Security

While servers deployed in a data center environment can benefit from the physical security of a centralized location, the same cannot be said for departmental servers, which are typically deployed in remote locations or distributed fashion, without the glass walls and secured badge access that a datacenter typically provides.

IBM understands that deploying servers into remote or distributed environments can expose them to physical threats not commonly associated with rack servers deployed into a datacenter. It was with this understanding in mind that IBM incorporated several significant physical security features into our latest generation of servers and chassis.

For example, the **BladeCenter Office Enablement Kit** (OEK) for the BladeCenter S chassis houses up to six blade servers, four communication switches, and a dozen drives containing up to 12TB of proprietary data (with another 4U of space available for other servers and rack equipment). BladeCenter S runs on standard 110V power and is designed for office use, making its drives a tempting target for thieves. To thwart physical access, the OEK provides locking doors for the front and back of the 11U (24 inches in overall height) enclosure. This protects the drives, switch modules, power supplies, and other equipment from theft. (Also standard is an acoustic module that dampens noise so that the OEK is office-friendly.)

Current tower servers include locking covers that protect the internal components but do nothing for front-removable hot-swap and simple-swap drives. Future System x tower servers will have locking covers that all lock the front bezel, thus protecting the drive bays as well.

Similarly, because even trusted data center employees aren't always trustworthy, IBM racks include locks for the front and back doors and side panels.

Some of the IBM products for System x and BladeCenter that offer enhanced physical data security include:

IBM System Storage™ DS8000 Series with Full Disk Encryption and Key Management

This innovative, self-encrypting disk array solution secures all information on disk drives when physically removed from the system. You no longer have to worry about the sensitive data on drives that are returned for repair, retired, or repurposed. Data is automatically protected against unauthorized access.

IBM System Storage DR550 with Encryption and Key Management

The DR550 is designed to provide a secure, scalable and cost-effective information retention solution, with support for data encryption. Archiving with the IBM System Storage DR550 can help companies address their data growth challenges, manage data throughout its life cycle, while reducing the cost of storing data over the long-term. The DR550 maintains data as nonerasable and nonrewritable until deletion is permitted by retention policy. It can manage the encryption keys for the tape encryption capabilities offered with System Storage TS1120, TS1130, and LTO-4® tape drives. The encryption on the tape drives is designed to allow for encryption within the drive and encryption key management independent of the application.

IBM System Storage TS1130 Tape Drive with Encryption and Key Management

This high-performance tape drive features flexible storage capability with support for data encryption, to help you establish easy access to data, better security, long-term retention and data governance and regulatory compliance.

IBM System Storage TS2900 Tape Autoloader with Encryption and Key Management

Entry-level tape storage solutions utilize the newest generation of IBM Linear Tape-Open (LTO®) technology to deliver exceptional performance and availability. The System Storage TS2900 Tape Autoloader provides plug-and-play and direct-attach capability to make it easy for you to manage your backups with limited resources. Onboard encryption also offers data security.

IBM System Storage TS3100 through TS3500 Tape Library with Encryption and Key Management

These tape libraries are designed to address capacity, performance, data protection, reliability, availability, affordability and application requirements. They are functionally rich, tape-storage solutions incorporating LTO Ultrium® tape technology, and are excellent solutions for large-capacity or high-performance encrypted tape backup, with or without random access.

IBM Virtualization Engine™ TS7530

The TS7530 solution is a high-performance, high-capacity open systems virtual tape solution designed to augment the tape backup and restore process in large tape environments. It supports TS1120 tape drive encryption and IBM LTO-4 drives and libraries. With support for up to 4,096 virtual tape drives and 512 virtual tape libraries, each backup server can be allocated its own virtual resources, allowing multiple and disparate backup applications to use the same physical resources. This offers the potential for infrastructure simplification. Various multiple tape libraries and tape drives can be aggregated to one or more TS7530s, helping centralize the backup resources and further reduce operational costs.

IBM Tivoli Key Lifecycle Manager

IBM extends its successful self-encrypting tape drive strategy to include self-encrypting disk solutions. Key Lifecycle Manager software manages encryption keys for self-encrypting disk and tape solutions, helping to simplify deployment and maintain data availability. It can enhance data security while dramatically reducing the number of encryption keys to be managed. It also helps facilitate compliance management of regulatory standards such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA).

Storage and Client Virtualization

Virtualization has garnered much attention lately as a way to consolidate servers to save data center space and lower energy and cooling bills. But it also offers benefits in the area of data security. Consolidating data from many departmental servers into a secure data center offers increased security. To this end, IBM storage virtualization tools can help transform the economics of enterprise storage by enabling you to simplify your infrastructure, protect your data and efficiently manage information. IBM **System Storage** tools allow you to virtualize disk and tape storage. Solutions include the **System Storage SAN Volume Controller**, **SAN File System**, **IBM Tivoli® Intelligent Orchestrator** and **IBM Tivoli Provisioning Manager**.

Another potential security exposure is user desktops. With local disk drives, user data, passwords, and other personal and corporate information is at risk. Virtualizing the client desktop is another approach to securing this data. To this end, IBM's **Virtual Client solution** allows users to enjoy all of the benefits and personal control of a stand-alone desktop—including print capabilities, USB drive support, and audio—while reducing many of the challenges related to current stand-alone desktop environments. These include limiting susceptibility to theft and viruses, ease of deployment of new users, limiting downtime during a hard drive failure, and eliminating the need for users to rebuild their preferences and settings after each client “refresh.”

Summary

Whether you are looking for the safest, most secure storage possible for your valuable passwords and keys, to encrypt critical business and private customer data, or to provide a high level of system security for your remote server deployments, IBM has employed the latest in state-of-the-art technologies and innovative server designs to provide you with the tools you need to meet your most stringent security environments.

For More Information

IBM System x Servers	**ibm.com**/systems/x
IBM BladeCenter Server and options	**ibm.com**/systems/bladecenter
IBM System x and BladeCenter Power Configurator	**ibm.com**/systems/bladecenter/powerconfig
IBM Standalone Solutions Configuration Tool (SSCT)	**ibm.com**/servers/eserver/xseries/library/configtools.html
IBM Electronic Service Agent	**ibm.com**/support/electronic
IBM ServerProven Program	**ibm.com**/servers/eserver/serverproven/compat/us
IBM Technical Support	**ibm.com**/server/support
IBM Configuration and Options Guide	**ibm.com**/servers/eserver/xseries/cog

Legal Information

IBM Systems and Technology Group
Dept. U2SA
3039 Cornwallis Road
Research Triangle Park, NC 27709

Produced in the USA
April 2009

For a copy of applicable product warranties, write to: Warranty Information, P.O. Box 12195, RTP, NC 27709, Attn: Dept. JDJA/B203. IBM makes no representation or warranty regarding third-party products or services including those designated as ServerProven or ClusterProven. Telephone support may be subject to additional charges. For onsite labor, IBM will attempt to diagnose and resolve the problem remotely before sending a technician.

IBM, the IBM logo, the e-business logo, BladeCenter, ServeRAID, System Storage, System x, Tivoli, and Virtualization Engine are trademarks of IBM Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://**ibm.com**/legal/copytrade.shtml.

Intel, Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

LTO, LTO-4, and Ultrium are registered trademarks of International Business Machines Corporation, Hewlett-Packard and Certance.

Microsoft, Windows, and Windows Server are trademarks or registered trademarks of Microsoft Corporation.

Other company, product and service names may be trademarks or service marks of others.

IBM reserves the right to change specifications or other product information without notice. References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates. IBM PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication may contain links to third party sites that are not under the control of or maintained by IBM. Access to any such third party site is at the user's own risk and IBM is not responsible for the accuracy or reliability of any information, data, opinions, advice or statements made on these sites. IBM provides these links merely as a convenience and the inclusion of such links does not imply an endorsement.

Information in this presentation concerning non-IBM products was obtained from the suppliers of these products, published announcement material or other publicly available sources. IBM has not tested these products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Some machines are designed with a power management capability to provide customers with the maximum uptime possible for their systems. In extended thermal conditions, rather than shutdown completely, or fail, these machines automatically reduce the processor frequency to maintain acceptable thermal levels.

MB, GB and TB = 1,000,000, 1,000,000,000 and 1,000,000,000,000 bytes, respectively, when referring to storage capacity. Accessible capacity is less; up to 3GB is used in service partition. Actual storage capacity will vary based upon many factors and may be less than stated.

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will depend on considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

Maximum internal hard disk and memory capacities may require the replacement of any standard hard drives and/or memory and the population of all hard disk bays and memory slots with the largest currently supported drives available. When referring to variable speed CD-ROMs, CD-Rs, CD-RWs and DVDs, actual playback speed will vary and is often less than the maximum possible.