Thinking Outside the Box

Monitoring DB2® Security on z/OS

January 2016

SDS
DO MORE WITH LESS

Thinking Outside the Box

Monitoring DB2® Security on z/OS

By Jerry Harding
Stephen D. Rubin
William Buriak

TABLE OF CONTENTS

Contents

1 Executive Summary

The United States recently introduced a universal healthcare system. This program requires the highly sensitive records to be stored on massive computers. Essentially, they will be a "DNA footprint" for millions of Americans. Security for these records should not be thought of as "after the fact" and will require vigilant and pro-active monitoring of security regardless of the host operating system.[1]

The records are required to be protected according to the Federal Information Security Management Act of 2008 (FISMA, also referred to as US Senate Bill S.3474). FISMA mandates that "the underlying framework that information systems and assets rely on in processing, transmitting, receiving or storing information electronically" have adequate security. It goes on to say, "Meaning security commensurate with the risk and magnitude of harm from loss, misuse, or unauthorized access to or modification of information".

Web connections to data residing on the mainframe DB2 platform through z/OS Web Services, CICS® and TSO® have added functionality to legacy processing and brought transaction processing to new levels. It has also introduced a new perception of vulnerability. Mainframe Security Administrators sometimes view it as opening up the mainframe to "intruders."

The "bad guys" are finding new inventive ways to obtain corporate and personal information and to disrupt a company's business as was done by someone holding the State of Virginia's medical records hostage and demanding a $10 million dollar payment.

Most of the Financial, Healthcare and Pharmaceutical industries keep their vital records on DB2 and other databases residing on the IBM z/OS mainframe platform. Government interests in these corporations will lead to the next wave of exchange of information among them and it is expected that private industries sharing database information with the Government will soon have to comply with the FISMA guidelines.

But regardless of the industry and whether or not they fall into the FISMA regulations, every company is at risk of losing information. Security is not always the highest priority in a corporation until it is named in the lead story

[1] Your medical information is worth 10-20 times more than your credit card number on the black market, according to a 2014 report by Reuters.

on the evening news or Wall Street Journal and you are requested to testify before Congress.

This paper puts its focus on ways to monitor z/OS DB2 database security by thinking outside the box. It will offer alternatives in developing an efficient security framework to monitor security settings and protect confidential data from 'bad guys' in an effective and economical manner. This paper will also explore the tools that are available for developing such a security framework. The main focus is placed on security tools that can be used outside the mainframe security framework. The stress on "thinking outside the box" is emphasized as the majority of the traditional tools that fall within the mainframe security setting have failed to meet today's security, auditing and compliance mandates. It will detail the steps to be taken when setting up log collection and security analysis programs on the mainframe by using economical sources readily available. However, along with mentioning the efficiency of this system, it will also put stress on the need for a new framework as very often traditional measures are found to be incapable of countering security threats of modern days. Finally it will discuss the methods that can be adopted to counter the latest security threats and how these tools work.

2 Background

Security teams for z/OS DB2 commonly use security products from IBM and Computer Associates for reporting. They are the first levels of defense. These products either allow or deny a user access to a resource. Unlike UNIX and other operating systems security, it is a simple yes or no decision. If security is denied, a violation event will be recorded on the security log files and in most cases a message will be issued to the primary console. The event may go unnoticed until the System Administrator runs a violation report in response to an incident.

DB2 is capable of keeping a separate log file of events throughout its course of normal processing. These log files are a mainframe operating system function called System Management Facility or "SMF®" records. The DB2 SMF records contain information related to many different types of events occurring within the system. The level of granularity depends on configurations of the DB2 audit trace at the individual table level. The SMF records provide data useful for investigating security events and if used in combination with other resources, help investigate possible attacks and breaches for incident response, auditing and compliance purposes. The DB2 SMF records are created in binary format and are not readable by a plain text editor, making online viewing and interpretation almost impossible.

Separation of Duties
One of the most fundamental aspects of the Sarbanes-Oxley Act of 2002 was the definition of Separation of Duties. Having the same person monitoring security and setting up security is a clear case of a violation of the Act.

The Evolving Security Function
The Security Administrators in most z/OS environments are responsible for monitoring security. In addition to defining and maintaining users and passwords, they assume the role of chasing down batch reports to answer periodic security, auditing and compliance questions.

Some leading mainframe installations are creating independent departments to actively monitor the security using SMF event information. Other installations are placing z/OS security into totally autonomous security groups that monitor Network, UNIX, Windows and other operating systems. Restructuring the mainframe security group (a) allows mainframe events to be monitored from "outside the box" in a centralized repository, (b) introduces new technologies and experience to mainframe computer security experts wishing to expand their careers, (c) allows non-mainframe security technicians to become exposed to what is happening "inside the box", and is a win/win proposition for the entire organization.

3 The Cost of a Data Security Breach

According to a 2015 study by the research organization Ponemon Institute, paid for by International Business Machines Corp., the cost of a data breach increased 23% since 2013. The total average cost of a data breach is now $3.8 million, up from $3.5 million a year ago

The study also reports that the cost incurred for each lost or stolen record containing sensitive and confidential information increased six percent from a consolidated average of $145 to $154.

Average figures don't paint a complete picture. If we look at one large retails loss, you can see the significant impact.

Target said the gross expenses from the data breach were $252 million. If you subtract insurance reimbursement, the losses fall to $162 million. Tax deductions lower the net losses tally $105 million. Still a significant loss!

Target's losses attributed to data breach				
	Gross expenses	Insurance reimbursement	Pre-tax net expenses	Net of tax expenses
2013	$191m	$46m	$145m	$94m
2014	$61m	$44m	$17m	$11m
Total	**$252m**	**$90m**	**$162m**	**$105m**

Beyond the financial implications a compromise of this nature would also include damage to corporate reputation, loss of customers, and increased regulatory scrutiny let alone the personal damage to the CIO and CEO

3.1 Personal Liability

Information security breaches may go beyond corporate boundaries and expose the corporation to unwanted legal actions. Security exposures derived from the theft of data has led to three class action law suits against the Secretary of Veterans Affairs. The theft was a result of data being transferred to a laptop which was later stolen from a private residence of a VA Contractor. The security breach affected 26.5 million records with a VA estimate of between $100 million and $500 million to prevent and cover possible losses from data theft.

3.2 The Regulators Cometh

It is bad enough that you had a data breach, the CEO was canned, and customers hate you. The real pain is only about to begin if your company happens to be in a regulated industry because security breaches reflect poorly on the regulators. They will push for more regulations and greater control. Everything will be verified and checked in great detail for years to come. Gone will be the reasonable assurance and all items will be looked into. Providing data to the regulators, responding to requests, and correcting issues, even minor ones is extremely time consuming and costly.

4 The Real Security Exposure to DB2 on z/OS

The most sought after target when attacking DB2 data on the mainframe is to acquire the privilege settings of the DB2 System Administrator. Compromising it and escalating the DB2 privileges to a common user's ID allows you to attack the DB2 data virtually unnoticed. It is becoming more difficult to do this in the modern days of DB2; however, an emphasis should be placed on monitoring accesses to critical information regardless of whether an individual has or does not have the correct privileges. It is not always safe to assume that a mainframe security product will always protect you.

One very good example of this occurred during the performance of a network vulnerability assessment at a large government agency. The network was compromised (with authority of the agency) and a workstation was hacked. Application files related to a process running on the workstation were examined. A mainframe unencrypted DB2 logon ID and password were found. The ID and password were then used to log into the DB2 application on the mainframe with SYSADMIN privileges. This was just an exercise, but if real the damages would be unlimited.

5 Weaknesses in DB2 Application Code

There are two major concerns regarding DB2 application code being developed and running on mainframe processors.

1) Random checks of application code being developed using mainframe Web Services seems to be in line with the security guidelines and standards of today but "you don't know what you don't know". Application reviews by the mainframe ISSO are almost non-existent.

2) Many of the DB2 legacy applications were written prior to the 9/11 mentality when it was not cost-justified to change them to fit into the security conscious world we are living in today. The inability to adapt these applications to today's security awareness posture poses a big problem for many large companies and government agencies around the world. Especially when one considers that the DB2 Data-warehouse containing the key corporate asset 'data' is updated, scanned, accessed continuously supporting critical business transactions. There reside the customer files, medical information, credit card records, social security data, financial records, etc., all prime targets for illegal information security breaches. The Government has responded with strict regulations under HIPAA, SOX and Graham Leach, along with financial penalties to corporate officers who fail to comply. Under these pressures it is time for corporate management to raise the bar for security methodologies protecting DB2 on z/OS to the highest level

6 Using DB2 SMF Records as Event Tracking

There are over 100 different types of SMF records reserved by the z/OS operating system for various operational functions. Record numbers above a certain level can be used for vendor products and mainframe application programs. SMF record number eighty (type 80 records) are used by two of the mainframe security products commonly found on the mainframe. A third security product uses an SMF number assigned to it at the installation time of the product (commonly # 231) and DB2 auditing uses SMF record type 102. The SMF records are written to files after the mainframe operating system performs an event. The mainframe Systems Programmer is responsible for defining the size of the primary and secondary SMF files. When the primary file fills, the secondary becomes the primary and the original SMF file is archived.

Common to all companies are thousands upon thousands of SMF records that are written daily and in many shops the SMF logs switch once a day, twice a day or perhaps hourly, depending on the customer's transaction processing volume. The volume of SMF records created cause major difficulties making it impossible to monitor the high volume from one workstation in real-time. Another problem presented is that these SMF records are typically made available with time lags between reports. So for example if batch reporting on DB2 SMF records by a bank are used to protect it from a security breach against credit card information and they are only available at best, on hourly increments, it presents a window of opportunity for a breach.

Another problem regarding batch reporting on SMF records is that these historical foundations for security, auditing and compliance batch reporting are not at all cost effective. In fact, the cost of manually reviewing logs is very high. Creation of logs with an aim to provide security is one thing, but actually manually reviewing and printing them is very expensive. Often companies seem to be reluctant in spending huge sums on reviewing these logs. But if a company does not review a log, then what is the purpose of putting efforts in collecting them?

7 How to Implement DB2 SMF Audit Trace Records

SMF log analysis is very important when it comes to monitoring DB2 security, auditing and compliance. One of the best ways to do it is by using the DB2 audit trace facility. The DB2 audit trace facility must be turned on for each table you wish to monitor. This is done by using the AUDIT clause at the time of the CREATE of the table. Additionally, Audit Trace classes must be activated in order to collect the data in the DB2 SMF records. Each class is associated with the type of DB2 events you wish to monitor. The DB2 Audit Trace Classes are as follows:

Class One

Access attempts that DB2 denies because of inadequate authorization.

Class Two

Explicit GRANT and REVOKE statements and their results. This class does not trace implicit grants and revokes.

Class Three

CREATE, ALTER, and DROP statements that affect audited tables, and the results of these statements.

Class Four

Changes to audited tables.

Class Five

All read accesses to tables that are identified with the AUDIT ALL clause.

Class Six

The bind of static and dynamic SQL statements of the following types:
INSERT, UPDATE, DELETE, CREATE VIEW, and LOCK TABLE statements for audited tables. SELECT statements on tables that are identified with the AUDIT ALL clause.

Class Seven

Assignment or change of an authorization ID because of the following reasons:

- Changes through an exit routine (default or user-written)
- Changes through a SET CURRENT SQLID statement
- An outbound or inbound authorization ID translation
- An ID that is being mapped to a RACF ID from a Kerberos security ticket

Class Eight

The start of a utility job, and the end of each phase of the utility.

Class Nine

Various types of records that are written to IFCID 0146 by the IFI WRITE function.

Class Ten

(DB2 V9.1) CREATE and ALTER TRUSTED CONTEXT statements, establish trusted connection information and switch user information.

Here is a partial list of DB2 security related events commonly monitored:

- Access rights
- Privilege changes, explicit privilege changes as well as administrative changes
- SYSCTRL and SYSADM activity
- Changes to authorization
- Dropping of tables
- Inserting/changing records
- Accessing data from unauthorized ID's
- GRANT/REVOKE statements

For some classes, other activity within the DB2 audit trail information, important for computer forensics and incident response, is the actual SQL statement that was being performed at the time of the incident. It is a fingerprint to the table, row and column that the user was going after at the time. Unfortunately, it is buried behind a very complex index of binary bit settings within the DB2 SMF audit trail record and difficult to interpret.

The DB2 Audit Trace facility is historically known for adding additional CPU overhead. DB2 has gotten progressively better when using this facility with each new release and there has been a drastic reduction on that overhead. The latest IBM statistics indicate that it will introduce less than 10% additional CPU overhead, per transaction, if all of the classes are turned on.

8 Thinking "Outside the Box"

The mainframe operating system platform is the premier transaction-processing machine and has always boasted industry-leading security technology. During many years of service, often under the most demanding conditions imaginable, it has survived. It has proven itself time and again, and was awarded the U.S. Government's highest certification for commercial security. However, in a changing world with an increase in lost trade secrets, theft of personal identity, and wrongdoings by employees, associates and contractors, the strongest security mechanisms are essential. The mainframe security concept of "allow" or "not allow" simply may not be enough. It needs additional safeguards that help protect users and data with features that were not possible until recently.

The answer to bringing mainframe security to the next level is; integrating mainframe "yes" or "no" security with existing network security products. The mainframe security professional needs the tools to accomplish this feat in a world where the Reagan-era motto "Trust but Verify" is essential. There are a variety of Log Management and SEIM products supporting DB2 that may already be deployed within your own organizations. These products sit outside the mainframe, on the network, and collect events logging from firewalls, UNIX, Windows and other operating systems. Very seldom does a mainframe Security Administrator tap into these resources.

8.1 Log Management

Log Management products are available from commercial vendors including LogLogic, Network Intelligence, Novell, Computer Associates, IBM and others. They are designed to collect raw log data. A partial mainframe solution is to route the console logs directly to the Log Management software. This is only a partial solution because the console logs alone do not contain all of the information required for fully monitoring the mainframe environment. A better approach to Log Management is to use the combination of raw data from console logs, security log files and SMF data. Problems arise when you attempt to send the combined information to the Log Management software because the volume of data traveling across the network creates a lag time. The information does not arrive in a "timely manner" as required by regulatory mandates as a result.

8.2 SEIM Products Supporting DB2

SEIM products collect security events from many sources other than the mainframe. The events are expected to be condensed by agent software executing on a remote device. DB2 SMF records can be excessive in length (the SQL could be 4k alone) and should be filtered or condensed for any SEIM product. The process of reading the security logs and condensing them into warnings and alerts is expected to occur by a remote agent process residing on the mainframe. Doing so saves network traffic overhead and expenses related to storing excess data in the central repository on a mid-range disk device. Commercial vendors for SEIM products such as NetIQ, Intellitactics, IBM, NetForensics, ArcSight and Novell often have remote batch or real-time process to collect DB2 information from the mainframe.

One way to leverage money already spent and to get the "employee of the month" award is to think outside the box and to integrate mainframe events into one of the products that your company has already invested in.

8.3 DB2 Mainframe Homegrown Solutions

Developing a homegrown agent application to read and monitor the DB2 SMF records, non-DB2 SMF records, console messages, application messages and vendor products is an overwhelming and monumental task. The DB2 SMF records are considered to be one of the most complex record formats and can only be interrupted by a veteran Systems Programmer. Not including the DB2 SMF records in a homegrown solution would produce a highly ineffective result.

Another interesting point is that the Sarbanes-Oxley Act of 2002 definition of Separation of Duties specifies that security personnel administrating or monitoring should not be writing security code. In essence, homegrown written code, including log monitors and exits written by a security person within the organization, is in violation of the very audit finding that it was intended to resolve.

With that being said; and you decide to proceed, there are some complicated technical and design issues that have to be worked out before you even begin. These issues include:

- Asynchronous timing
- Unacceptable consumption of CPU and Network resources
- Conversion of data from binary to text format
- Delivering the information on a timely manner so that it can be immediately acted upon.

The complexity and costs related to the development of a homegrown application is often cast aside by management when compared to the cost of purchasing proven software from reliably vendors.

9 Summary:

DB2 z/OS is here to stay and will only grow to accommodate data warehousing requirements and corporate business transactions. In the past the security emphasis always seemed to be on distributed systems. However the new Government regulations have leveled the field to include all data, as exampled under the Federal Information Security Management Act (FISMA) of 2008. Every Government computer and network is essentially required to protect its confidential data and any other types of records. These standards are about to spill over into the commercial arena with the fusion of Government and commercial entities. SOX and HIPAA have no computer boundaries regarding the compromise of critical data. Unauthorized changes to patient information or accounting records are all fair game in the eyes of the law.

In this paper we have addressed some important issues relating to security breaches. They include how the mainframe platform works towards monitoring security of records, what the pitfalls are in the traditional methods of using DB2 SMF records for event tracking, and how the mainframe platform can be modernized to provide improved security monitoring of important and confidential records. An attack, especially on DB2 z/OS to obtain the privilege settings of the DB2 System Administrator, allows for a stealthy security breach. Therefore, it is no longer efficient or safe to rely solely on batch reporting and mainframe security systems that work strictly inside the mainframe, only recording on incidents where security has been violated. It is now possible to use products to monitor mainframe security from outside the mainframe itself.

Among the various kinds of security products that can work sitting outside the mainframe platform are Log Management and SEIM (Security Event and Incident Management) products supporting DB2. Each of these products has their own pros and cons and there is no “one shoe fits all” solution. The important point is that all these solutions are more economical, efficient and faster than the earlier models in countering new types of security threats.

So, how will you choose the correct software among the many alternatives? While choosing a particular security product that is able to work sitting outside the mainframe platform, certain factors have to be checked. Here are some criteria that you may consider when evaluating a security product for your company:

- Scalable
- Ease of use
- Room for lateral growth
- Real time 24/7 event monitoring
- Ease of configuration and installation
- Small footprint of mainframe processing and minimum performance impact on mainframe systems

Although the cost of protecting data effectively is high, the cost of a security breach is even higher considering the new laws governing the compromise of data. Companies can take a sigh of relief now that there is cost effective and comprehensive mainframe software available in the market. These products meet the current needs of the corporations in the area of securing confidential records of their own businesses as well as of their clients, and have all the qualities that are required to counter today's security threats. They work efficiently with existing mainframe security products and make use of SMF and console messages in appropriate ways. They are capable of tracking DB2 audited events, several types of insider threats, delivering mainframe alerts in real time and easily integrating with other existing security monitors.

Proactive companies, having a track record of monitoring security logs from outside the box, are in the forefront of Government requirements and have a solid framework in place to manage DB2 data and its associated risks. Doing so puts them, regardless of their industry, in a better competitive position, with an ideal security posture that will allow them to participate in the very important data-sharing evolution taking place.

About the Authors:

Jerry Harding

Jerry Harding is CEO of Type80 Security Software, Inc. He has over 25 years of mainframe Systems Programming experience, providing professional services to commercial clients and government agencies. He also has over 15 years of security experience including providing training to NATO's Counterintelligence Agency (ACE CI), the Supreme Headquarters Allied Powers Europe (SHAPE), as well as other public and private organizations.

Stephen D. Rubin

Stephen D. Rubin is the founder and president of MMI. Under his leadership MMI has a track record of 20 years of financial success in creating business markets for information technology services (IT) across North America. Areas of business include training, consulting services, and software. MMI has trained over 3,000 IT students representing over 400 corporations in database design, information security, capacity planning and distributed application development. Professional service engagements have included information security, server consolidation, and the auditing of capacity planning and chargeback methodologies for both public and private sectors. Stephen has authored white papers to drive market recognition and helped create the United States marketplace for a European software start-up client.

William Buriak

William Buriak has over 25 years of information technology experience with an extensive background in financial services, healthcare, and technical and management consulting. Bill is a Senior Executive with demonstrated experience in planning, developing, and implementing cost effective, innovative solutions to address complex business problems. He has broad recognized experience in managing mainframe systems, Web based, and distributed systems. He has extensive qualifications including vendor management, consensus building, and strategic planning skills. Currently working in the Security Engineering area of a major world bank, Mr. Buriak is responsible for compliance and control of a large number of global products.

About SDS

Software Diversified Services (SDS) was founded in 1982, and now supports over 20 z/OS, MVS, VSE, and VM mainframe systems for more than 1,000 clients worldwide, as well as encryption for Windows, UNIX, Linux and AIX. PC software related to the mainframe industry is also available through SDS.

Our customers include many Global 500 companies in banking, ȧnance, insurance, and retail, as well as local, state, and national governments.

Security, encryption, and network management are our current focus, also performance monitoring, report distribution, and client-server applications.

At SDS, technical support works hand-in-hand with development. SDS is noted for having the highest quality software, documentation, and technical support in the business. SDS technical support has been rated number 1 by the prestigious IBEX Bulletin.

Software Diversified Services

1322 81st-Ave NE
Minneapolis, MN 55432-2116
Phone: 763-571-9000
info@sdsusa.com
www.sdsusa.com

SDS
DO MORE WITH LESS