DB2 Information Management Software

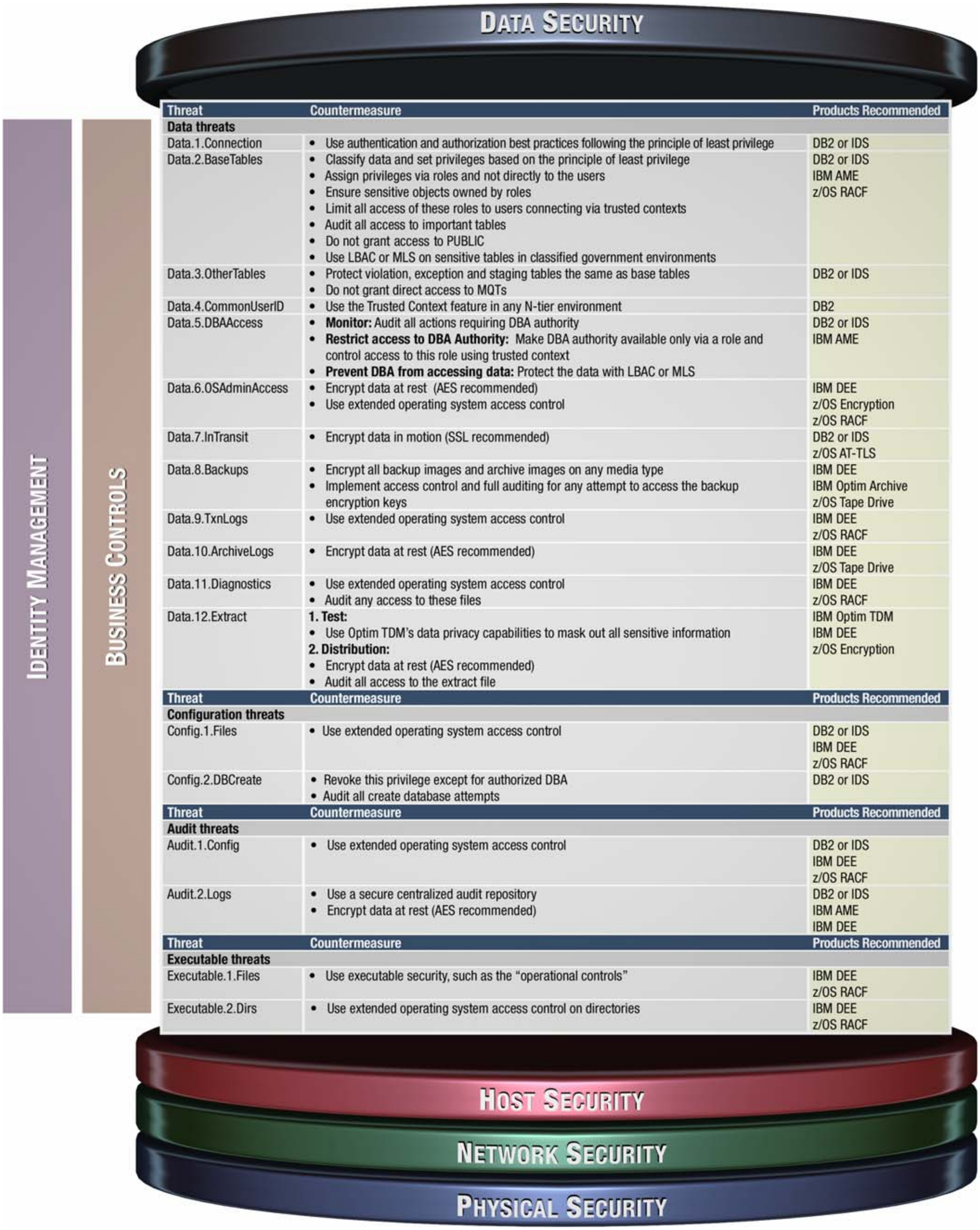
IBM Data Server Security Blueprint

March 2008

Belal Tassi, IBM Toronto Lab
Walid Rjaibi, IBM Toronto Lab
Paul Caliandro, Vormetric

Table of Contents

IBM DATA SERVER SECURITY BLUEPRINT – V1.0.0



Threat	Countermeasure	Products Recommended
Data threats		
Data.1.Connection	• Use authentication and authorization best practices following the principle of least privilege	DB2 or IDS
Data.2.BaseTables	• Classify data and set privileges based on the principle of least privilege • Assign privileges via roles and not directly to the users • Ensure sensitive objects owned by roles • Limit all access of these roles to users connecting via trusted contexts • Audit all access to important tables • Do not grant access to PUBLIC • Use LBAC or MLS on sensitive tables in classified government environments	DB2 or IDS IBM AME z/OS RACF
Data.3.OtherTables	• Protect violation, exception and staging tables the same as base tables • Do not grant direct access to MQTs	DB2 or IDS
Data.4.CommonUserID	• Use the Trusted Context feature in any N-tier environment	DB2
Data.5.DBAAccess	• **Monitor:** Audit all actions requiring DBA authority • **Restrict access to DBA Authority:** Make DBA authority available only via a role and control access to this role using trusted context • **Prevent DBA from accessing data:** Protect the data with LBAC or MLS	DB2 or IDS IBM AME
Data.6.OSAdminAccess	• Encrypt data at rest (AES recommended) • Use extended operating system access control	IBM DEE z/OS Encryption z/OS RACF
Data.7.InTransit	• Encrypt data in motion (SSL recommended)	DB2 or IDS z/OS AT-TLS
Data.8.Backups	• Encrypt all backup images and archive images on any media type • Implement access control and full auditing for any attempt to access the backup encryption keys	IBM DEE IBM Optim Archive z/OS Tape Drive
Data.9.TxnLogs	• Use extended operating system access control	IBM DEE z/OS RACF
Data.10.ArchiveLogs	• Encrypt data at rest (AES recommended)	IBM DEE z/OS Tape Drive
Data.11.Diagnostics	• Use extended operating system access control • Audit any access to these files	IBM DEE z/OS RACF
Data.12.Extract	**1. Test:** • Use Optim TDM's data privacy capabilities to mask out all sensitive information **2. Distribution:** • Encrypt data at rest (AES recommended) • Audit all access to the extract file	IBM Optim TDM IBM DEE z/OS Encryption
Threat	Countermeasure	Products Recommended
Configuration threats		
Config.1.Files	• Use extended operating system access control	DB2 or IDS IBM DEE z/OS RACF
Config.2.DBCreate	• Revoke this privilege except for authorized DBA • Audit all create database attempts	DB2 or IDS
Threat	Countermeasure	Products Recommended
Audit threats		
Audit.1.Config	• Use extended operating system access control	DB2 or IDS IBM DEE z/OS RACF
Audit.2.Logs	• Use a secure centralized audit repository • Encrypt data at rest (AES recommended)	DB2 or IDS IBM AME IBM DEE
Threat	Countermeasure	Products Recommended
Executable threats		
Executable.1.Files	• Use executable security, such as the "operational controls"	IBM DEE z/OS RACF
Executable.2.Dirs	• Use extended operating system access control on directories	IBM DEE z/OS RACF

INTRODUCTION

Your data is under attack.

You know what data we are talking about. Your customers' confidential addresses, their credit card numbers, their spending patterns, and their health records. Your employees' social security numbers, their salary information, and their performance scores. Your company's financial audit records and the sales data for the last 12 quarters. The designs of your core products, the sales and marketing plans for your upcoming product launch, and other critical intellectual property of your company. And a whole lot more.

In many ways, data security is priceless. No one can erase your company's name from the front page of the newspapers and undo the damage of a data security breach. Once your data is on the loose, it can't be reined back in.

This is the Information Age, and since information is power many people want access to that information – whether they are entitled to it or not. Many data breaches are perpetrated by those with malicious intent, either inside or outside your organization. More commonly, such as with the recent scandal from November 2007 in the UK where *Her Majesty's Revenue and Customs (HMRC)* lost a number of password protected but unencrypted data disks containing sensitive information about some 25 million families with children in the UK, data breaches are caused by negligence or lapse of judgment.

Of course, this does not come as news to those tasked with securing our computing environments for the past few decades. Theft, fraud, and malicious attacks have unfortunately been around for a long time – since long before the advent of computers or even the abacus, for that matter. In fact, the first known encryption method was developed by Julius Caesar to protect messages to and from his soldiers in the field. Information has always been valuable. However, what has changed is the sheer quantity of the data that is being generated and collected, the manner in which it is kept, and its new critical importance in running organizations of all types and ultimately modern society itself. As the information that we unlock from our data becomes more and more valuable, it should come as no surprise that malicious parties are increasingly interested in gaining access to this data. We thus see an increase in the frequency and impact of such attacks.

Like other complex, systemic problems in the real world, there is no such thing as a single "quick fix" for securing data. If things were that easy, the problems would have been solved by now and we would be living in a world full of secure data. There is no "silver bullet" to security. The best security IT professionals can attain is to make the process and cost of stealing data difficult and prohibitively expensive to would-be attackers.

Securing data requires a holistic and layered approach taking into consideration the broad range of threats. This is commonly referred to as *defence in depth*, a term adopted from military strategy. Defence in depth is a fundamental tenet for today's information security. It requires a "security by design" approach, which espouses security as part of the core design of database environments, the supporting infrastructures and business practices around these environments. This means building robust security components directly into the database and data storage environments from day one to enforce data security best practices. Multiple layers of security, each layer of which plays an important part in securing the system and is reinforced by other layers, are the underpinnings of an environment in which data is secure. Together these provide the three ultimate objectives of security, commonly known as the CIA triad: confidentiality, integrity, and availability.

IBM understands these data security threats, and designs comprehensive security directly into its data server products. Much of the industry's valuable data is currently being stored and managed in IBM's industry-leading flagship data servers: IBM® DB2® 9 and IBM Informix® Dynamic Server 11

(“IDS”) data servers. Both data servers feature comprehensive security and auditing capabilities to help protect even the most critical data in the data server.

The IBM Data Server Security Blueprint is a one-page diagram that enumerates the most common data security threats and outlines recommended countermeasures. Organized in a short easy–to-understand format, the IBM Data Server Security Blueprint provides a practical road map for users of IBM’s data servers in securing their data from some of the major data security threats that exist today. It outlines these threats and proposes countermeasures to address these threats.

This paper explains the IBM Data Server Security Blueprint in more detail, and provides the background and additional details about the selected threats and countermeasures proposed by the blueprint. Chapter 1 discusses why we need such a blueprint, and the role it plays in helping you begin to secure your data server. Chapters 2 and 3 describe the threats and proposed countermeasures outlined in version 1.0.0 of the blueprint. Chapter 4 provides an introduction to each of the security-enhancing products referenced in the blueprint. Chapter 5 concludes the paper with a summary tying the discussions together. Important additional information on the secure configuration and operation of IBM Data Server products are listed in the More Information section at the end of this document.

IBM DB2 and IBM IDS have long been industry leaders of the “SHARP” characteristics: Scalability, High Availability, Reliability, and Performance. With the increased importance of data server security and the security capabilities that IBM DB2 and IBM IDS bring to the table, we can add another important characteristic and henceforth update the acronym to **SHARPS**: Scalability, High Availability, Reliability, Performance, and **Security**.

CHAPTER 1: WHY A DATA SERVER SECURITY BLUEPRINT?

1.1 – Data Security is not trivial

The challenges facing those entrusted with securing data are not easy. At a minimum, rolling out an effective data security plan should always include the following seven steps:

1. **Data Classification:** First, you must understand and ultimately classify your data. Which parts of the data are most important, and which are less so? What is the value of the data to the organization? What is the cost if the data is compromised?

2. **User Classification:** After the data has been classified, you must determine who is allowed to access the data. What is the minimum level of authorities/privileges that employees need to do their jobs? How long does each employee need to have this level of authority/privilege? At this stage, the two security principles of least privilege and separation of duties are vital.

3. **Threat Identification:** You must understand the threats you are facing. The threats that you know about must be enumerated and categorized in a logical fashion. You must decide which threats apply to your environment and which ones (if any) do not. You must also do your best to anticipant, and be generally prepared for, unforeseen threats.

4. **Counter/Preventative Measures:** You should implement effective measures to address every threat deemed important in your environment. It makes little sense to buy a titanium front door to secure your house when the side door is made of wood – determined thieves will use the side door. In most cases, addressing threats will involve multiple layers – remember defence in depth. Lastly, these solutions should also be easy to deploy and manage; otherwise, no one will use them, or worse, people will think the solutions are applied properly when in fact they are not.

5. **Testing:** You should test and validate that your security mechanisms are in place and working properly. In many ways, this can be the hardest part; not only should your system be secure but there must be a way to continuously validate that it is so. This testing must be performed in a variety of ways – including both vulnerability (to detect any current vulnerabilities) and penetration testing (to test the effectiveness of applied countermeasures and the impact of a breach).

6. **Auditing:** You should be auditing and monitoring your system to provide a historical trail of data access and, ultimately, to detect any attempts to improperly access the data. Otherwise, as happens all too frequently, no one will be able to detect when a breach has occurred or something has gone wrong. Effective data security is an ongoing process, and auditing is the key feedback method in this process.

7. **Maintenance:** This brings us to the last and longest step of keeping everything maintained and secure. Effective security is not a point in time exercise: everything should be kept up to date as new threats are identified, new users are added, and your data environment changes as inevitably it will. Security maintenance should be integrated in your standard operational practices and people tasked with keeping it up to date as an important part of their core everyday responsibilities.

1.2 – How the Blueprint Helps

To help simplify the task of implementing proper data server security, we have created the IBM Data Server Security Blueprint to be used as a road map to assist in rolling out proper security mechanisms in your own shop.

This blueprint has arisen out of multiple customers' inquiries about how they can ensure they are "covered" from the standard data security threats, and some not-so-standard threats. Included are the most common data threats with the proposed countermeasures to adequately address these threats. The proposed countermeasures are all current best practices as recommended by the security teams for each data server, and are using IBM Information Management products and features that are all available as of the date of publication of this document.

1.3 - Assumptions and Prerequisites

Technology comprises interdependent components. Security must exist on each of these components at each layer in the environment to make a truly secure system. The IBM Data Server Security Blueprint focuses on the database tier and the underlying data level security. It assumes that the overall environment that the Data Server runs in is also being properly secured. Specifically, it assumes that the following security layers and processes *are already in place in the environment:*

- **Network Security**: Firewalls, Virtual Private Networks (VPN's), secure routers, intrusion detection systems, detecting network sniffers, and so on.

- **Host Security:** Securing the operating system, virus and malware protection, Web browser security, monitoring and logging activities of privileged system users, and so on.

- **Physical Security**: Effective badge access controlling who can physically access the machine(s) hosting the Data Server.

- **Identity Management:** Reliable systems and methods for identifying and authenticating enterprise users effectively.

- **Business Controls:** Rules, processes and practices governing access to assets and the use and management of data.

CHAPTER 2: THREATS

You should know what type of threats you are up against. The blueprint divides the data server security threats into four broad categories: Data Threats, Configuration Threats, Audit Threats, and Executable Threats.

Data Threats: Threats against data are mechanisms whereby data can be accessed by users or processes that are not authorized to access such data. This is by far the largest category of threats, and is usually the first that come to mind. These threats can be aimed directly at the tables in the database, or through more indirect means such as by looking at the log files or directly at the table space files on the operating system.

Configuration Threats: Threats against configuration mechanisms whereby the database or database manager configuration files can be tampered with. Since they control critical aspects of your data server – such as how and where authentication is performed – it is critical that the database configuration files are protected as securely as the data itself.

Audit Threats: Threats against the audit facility are mechanisms whereby the audit configuration, audit logs, or archive logs can be tampered with. In many cases, audit records are the only way to determine what has happened in the past and the only form of evidence to detect misuse; it is critical that they be able to withstand tampering.

Executable Threats: Threats against executables are mechanisms whereby database manager executable files can be tampered with. This includes executable spoofing, denial-of-service attacks and Trojan horse attacks.

In the following sections, each threat is uniquely identified by a three-part name: the category followed by a unique number, and one word identifying the threat.

This always takes the form:

<category>.#.<threat short name>

For example, the threat **Data.6.OSAdminAccess** is threat #6 in the “Data” category and is referenced by the short name “OSAdminAccess”.

2.1 – Data Threats

Threat	Threat Description	Explanation
Data.1.Connection	Exploiting poor database connection authentication and authorization	An unauthorized user can exploit poor authentication practices on the database to connect to the database. The most common examples of these practices include requiring no server-side credentials to authenticate users when connecting (e.g., using the CLIENT-side authentication), or by granting the CONNECT privilege to the group PUBLIC.

Threat	Threat Description	Explanation
Data.2.BaseTables	Exploiting poor authorization controls on base tables	An unauthorized user can exploit poor authorization practices in the database to access data on the base tables and system catalog tables. For example, leaving the group PUBLIC with access to the system catalog tables allows any user to access all their information.
Data.3.OtherTables	Exploiting poor authorization controls on replicated tables, Materialized Query Tables (MQTs), staging tables, exception tables, and OLAP Cubes	An unauthorized user can exploit poor authorization practices on the database to access data on other important non-base tables. These tables include: ➔ SQL Replicated tables ➔ MQTs ➔ Exception tables ➔ Staging tables ➔ OLAP Cubes ➔ Clone Tables
Data.4.CommonUserID	Loss of identity of connected users in N-tier architectures due to common user ID	Application servers often use a common user ID to connect to the database that works on behalf of all its applications. This common user ID weakens user accountability and the ability to properly audit database access. This also leads to over-granting of privileges to this common user ID, effectively bypassing most database privilege checking.
Data.5.DBAAccess	Abusing database administrator privileges	By default DBAs have access to any table in their database. A privileged database administrator – or those who unlawfully acquire database administrator authority – can abuse that privilege by reading or modifying data that they should not be seeing. This is a critical component of “insider abuse”.

Threat	Threat Description	Explanation
Data.6.OSAdminAccess	Abusing operating system administrator privileges	Both a user with OS administrator privileges and the instance owner of the database have direct file system access to OS files where table data resides. They can abuse that privilege by directly reading or copying the contents of these files via the file system and bypass access controls placed inside the database. This is a critical component of “insider abuse”.
Data.7.InTransit	Sniffing data in transit on the network	Data, user ids and passwords traveling in clear text over a network can be viewed by network sniffers.
Data.8.Backups	Exploiting poor security on backups and archives	Many times unauthorized access to data occurs once the data has left the protection of a running data server environment. If left unprotected, data can be accessed directly from backup and archive images, whether left onsite or put offsite for disaster recovery (DR) purposes.
Data.9.TxnLogs	Exploiting poor security on transaction logs	Transaction logs contain valuable data that can also be exploited – such as inserted data values. Since they are just files on the file system, transaction logs can be accessed directly by the OS administrator on the production system. Also if transaction logs are mirrored or replicated, these copies can also be exploited by a privileged user as well.
Data.10.ArchiveLogs	Exploiting poor security on archived transaction logs	Archived transaction logs contain valuable data that can also be exploited – such as inserted data values. Once transaction logs are archived for recovery purposes, they usually leave the protection of the production system and are put on other servers or devices. Privileged users on those archive servers or devices can abuse their privileges and access data within these archived transaction logs.

Threat	Threat Description	Explanation
Data.11.Diagnostics	Exploiting poor security on trace files, dump files, and output of monitoring and diagnostic tools	Many diagnostic logs, monitoring output, and dump files contain valuable information that can be exploited by attackers. For example, data in the diagnostic logs and trace files can contain data values and are logged in clear text. Also, unloading of the direct raw page images from tables directly to disk can easily be done using tools such as **db2dart** or IDS **onunload**. This dumped data provides an indirect means to view data in the data server.
Data.12.Extract	Exploiting extracted data that has been moved from its secure home	Data is commonly extracted from the production environment into an export file or another database, usually for distribution or test purposes. Once it is extracted, it leaves the security of the data server environment and is often left exposed to unauthorized access. This is also true for load input files that are waiting to be loaded into a data server. This threat can be split into two cases according to the ultimate goal of the extraction: **1.** **Test:** When the data is being used in test environments, the data must have the same properties as production data but can safely be masked or changed to preserve sensitive data such as credit card numbers or social security numbers. **2.** **Distribution:** When the data is being extracted for distribution to another location, the data must be left identical to that in production. This includes data extracted by Extract, Transform and Load (ETL) processing and those for replicated tables.

2.2 – Configuration Threats

Threat	Threat Description	Notes
Config.1.Files	Exploiting poor security on database configuration files	If the DBMS configuration files are insecure, an intruder can modify the way the system behaves and make it reveal information that should not be revealed.
Config.2.DBCreate	Exploiting lack of authorization controls on who can create databases	Creating a database in a database management system is a privileged operation that is controlled by the instance configuration. Only trusted users should be authorized to

Threat	Threat Description	Notes
		create a database within an instance.

2.3 – Audit Threats

Threat	Threat Description	Notes
Audit.1.Config	Exploiting poor security on audit configuration files	Unauthorized personnel should not be able to alter the auditing behavior on the system. This is a common way for attackers to hide their tracks *before* performing an unauthorized breach. Unauthorized personnel should not be able to modify the audit configuration files.
Audit.2.Logs	Exploiting poor security on audit log files	Audit logs contain valuable data that can be exploited – both from the perspective of modifying past auditing results and of understanding data server access patterns for would-be attackers. This is a common way for attackers to hide their tracks *after* performing an unauthorized breach. Unauthorized personnel should not be able to alter or view the audit records or archived audit records.

2.4 – Executable Threats

Threat	Threat Description	Notes
Executable.1.Files	Maliciously modifying data server executable files	Data server executable files can be maliciously modified, for example by adding an identically named version containing a Trojan horse, or completely removed to perform a denial-of-service attack. Also executables and libraries used by stored procedures and UDF's can also similarly be maliciously modified. Only the user entrusted with installing the software should be able to modify the executables used by the data server.
Executable.2.Dirs[1]	Exploiting poor security on directories containing executables or data	If the directories containing the executables or the data files are not secure, then attackers could modify directory paths to mount a denial-of-service attack on the database system.

[1] This threat is not applicable on z/OS systems

CHAPTER 3: RECOMMENDED COUNTERMEASURES

Effectively protecting your database from the threats outlined in Chapter 2 demands effective organizational processes and controls as well as technical components. Your protection plan must include both aspects. Implementing only one aspect will likely leave you vulnerable to attacks by determined individuals with malicious intent or to negligent mistakes. Such an approach is analogous to locking the doors and leaving the windows open.

The tables below document the *technical components* of the **recommended countermeasures** to address each of the aforementioned threats. The recommended countermeasure is presented followed by the features and solutions needed to implement the recommended countermeasure using the latest product version as outlined in Chapter 4.

The following products and associated short names are utilized in this document:

Linux®, UNIX®, and Windows® Platforms:

Products	Short name
DB2 for Linux, UNIX, and Windows (LUW)	DB2
Informix Dynamic Server (IDS)	IDS
IBM Database Encryption Expert	IBM DEE
IBM Audit Management Expert	IBM AME
IBM Optim Test Database Management	IBM Optim TDM
IBM Optim Archive	IBM Optim Archive

z/OS® Platform:

Products	Short name
DB2 for z/OS	DB2
IBM Audit Management Expert for z/OS	IBM AME
IBM Optim Test Database Management	IBM Optim TDM
IBM Optim Archive	IBM Optim Archive
z/OS Security Server (Resource Access Control Facility, RACF®, or equivalent)	z/OS RACF
IBM Data Encryption for IMS and DB2 Database tool	z/OS Encryption
z/OS Communication Server Application Transparent Transport Layer Security	z/OS AT-TLS
IBM System Storage™ TS1120 Tape Drive	z/OS Tape Drive

3.1 – Data Threats

Threat	Threat Description	Countermeasure	Products Recommended
Data.1.Connection	Exploiting poor database connection authentication and authorization	Use authentication and authorization best practices following the principle of least privilege.	DB2 or IDS

Threat	Threat Description	Countermeasure	Products Recommended
Data.2.BaseTables	Exploiting poor authorization controls on base tables	ALL OBJECTS - Set proper database privileges and access controls based on data sensitivity classification and principle of least privilege. - REVOKE all privileges from those who do not absolutely need them. - Assign privileges to roles and not directly to specific users. - Have sensitive objects owned by roles and limit all access of these roles to users connecting from trusted contexts. - When creating new database objects, ensure access is never granted to PUBLIC. BASE or SYSTEM CATALOG TABLES - Audit all access to important tables - When possible, make sure access to the system catalogs is not granted to PUBLIC - The use of Label-Based Access Control (LBAC) or z/OS MLS on sensitive tables is recommended in government and other highly sensitive and regulated environments.	DB2 or IDS IBM AME z/OS RACF

Threat	Threat Description	Countermeasure	Products Recommended
Data.3.OtherTables	Exploiting poor authorization controls on replicated tables, Materialized Query Tables (MQTs), staging tables, exception tables, and OLAP Cubes	- Violation, exception, and staging tables should be fully protected against unauthorized access, just as the corresponding base tables are. - MQTs serve as a results set cache for improving query performance (via MQT routing). As such, MQTs should be regarded as internal tables, and users should not be given direct access to them. - If direct access to the MQT is required, turn on fine-grained auditing of all SQL access to the MQT.	DB2 or IDS
Data.4.CommonUserID	Loss of identity of connected users in N-tier architectures due to common user ID	- Use the Trusted Context feature in any N-tier environment. Trusted contexts allow the middle-tier to assert the identity of the end user accessing the database. The end user's database identity and database privileges are then used for any database requests by that end user.	DB2
Data.5.DBAAccess	Abusing database administrator privileges	- **Monitor:** Audit all actions requiring DBA authority. - **Restrict access to DBA Authority:** Assign DBA authority only through a role and control access to this role using trusted contexts. This will restrict access to only trusted connections originating from trusted hosts. - **Prevent DBA from accessing data:** Protect the data with LBAC or z/OS MLS features.	DB2 or IDS IBM AME

Threat	Threat Description	Countermeasure	Products Recommended
Data.6.OSAdminAccess	Abusing operating system administrator privileges	- Prevent the data from being copied or read directly from the file system by using disk encryption. AES encryption is recommended. - Prevent sensitive files, such as the table space files, from being modified directly by the OS administrator. This requires **extended OS access control** functionality, such as that provided by IBM DEE and z/OS RACF.	IBM DEE z/OS Encryption z/OS RACF
Data.7.InTransit	Sniffing data in transit on the network	- Encrypt the data before it is transferred on the wire. - In most cases, the recommendation is to use SSL encryption[2]	DB2 or IDS z/OS AT-TLS
Data.8.Backups	Exploiting poor security on backups and archives	- Encrypt *all* backup images and archive images on *any* media type (disk, tape, etc.). - Restoration of the backup image must require controlled access to the encryption key and must be audited.	IBM DEE IBM Optim Archive z/OS Tape Drive
Data.9.TxnLogs	Exploiting poor security on transaction logs	- Prevent files from being modified directly by the OS administrator or any other user using extended OS access control.	IBM DEE z/OS RACF
Data.10.ArchiveLogs	Exploiting poor security on archived transaction logs	- Prevent the logs from being copied or read directly from the file system by using disk encryption.	IBM DEE z/OS Tape Drive

[2] Turning on network encryption will cause any third-party data sniffing application to no longer function.

Threat	Threat Description	Countermeasure	Products Recommended
Data.11.Diagnostics	Exploiting poor security trace files, dump files, and output of monitoring and diagnostic tools	- Prevent files from being modified directly by the OS administrator or any other user using extended OS access control. - Audit any direct file system access to these files.	IBM DEE z/OS RACF
Data.12.Extract	Exploiting extracted data that has been moved from its secure home	- Countermeasure depends on the reason the data is being extracted: **1. Test:** Use Optim Test Data Manager's data privacy capabilities to automatically mask out all sensitive information from the data during extraction to your test environment. **2. Distribution:** Prevent extract file from being read or modified by using disk encryption. Audit all access to the extract file.	IBM Optim TDM IBM DEE z/OS Encryption

3.2 – Configuration Threats

Threat	Threat Description	Countermeasure	Products Recommended
Config.1.Files	Exploiting poor security on database configuration files	- Prevent files from being modified directly by the OS administrator or any other user using extended OS access control.	DB2 or IDS IBM DEE z/OS RACF
Config.2.DBCreate	Exploiting lack of authorization controls on who can create databases	- Revoke this privilege except for authorized DBA. - Audit all create database attempts.	DB2 or IDS

3.3 – Audit Threats

Threat	Threat Description	Countermeasure	Products Recommended
Audit.1.Config	Exploiting poor security on audit configuration files	- Prevent files from being modified directly by the OS administrator or any other user using extended OS access control.	DB2 or IDS IBM DEE z/OS RACF
Audit.2.Logs	Exploiting poor	- Use a secure centralized audit	DB2 or IDS

	security on audit log files	repository such as IBM AME. - Use extended OS access control to prevent files from being modified directly on file system by the OS administrator or any other user. - Encrypt the audit logs records on disk.	IBM AME IBM DEE

3.4 – Executable Threats

Threat	Threat Description	Countermeasure	Products Recommended
Executable.1.Files	Maliciously modifying data server executable files	- Use executable security feature, such as the “operational controls” functionality in IBM DEE, to prevent executable modification.	IBM DEE z/OS RACF
Executable.2.Dirs	Exploiting poor security on directories containing executables or data	- Use extended OS access control to prevent directories from being modified by unauthorized users.	IBM DEE z/OS RACF

CHAPTER 4: PRODUCT OVERVIEWS

4.1 – IBM DB2 9.5 for Linux, UNIX, and Windows

The DB2 for LUW (“DB2”) software security capabilities can be divided into four broad areas: authentication, authorization, encryption, and auditing.

Authentication is the first security capability encountered when a user attempts to use DB2. The user must be identified and authenticated before they are allowed to use any of the DB2 services. DB2 relies on a security plug-in architecture for authentication. The security plug-in determines where authentication takes place, which is generally the operating system but it can also be Kerberos or an LDAP server.

Authorization is the next security capability encountered. The authenticated user must be authorized to perform the action they are attempting. Authorization can be coarse-grained (for example, at a table level) or fine-grained (for example, at a row or column level). For a given operation, DB2 checks whether or not the user’s permissions are sufficient to allow them to carry out that operation. Users can acquire permissions either directly or indirectly through membership in roles and groups.

Encryption can be employed to keep information confidential when it is transmitted between a DB2 server and a DB2 client or when it is stored on disk. For data transmission confidentiality, DB2 provides two options: The native DATA_ENCRYPT capability and Secure Sockets Layer (SSL). For data storage, there are also two options: the native encryption and decryption column functions and the IBM Database Encryption Expert. It is highly recommended to use IBM Database Encryption Expert as this provides more security, better performance, and most importantly requires no application-level changes.

Lastly, the audit facility can be turned on to track user actions. For example, the security administrator can consult the audit trail to find out what actions a particular user executed in a given timeframe. In DB2 9.5, the audit facility has been substantially improved to provide finer granularity and to reduce the auditing performance overhead.

Label-Based Access Control (LBAC) has also been enhanced so that security administrators can assign security labels and exemptions to roles and groups. DB2 9.5 also provides a new security capability that helps address the security concerns that arise from the use of a single user ID to access the database in three-tier environments. This capability is referred to as *trusted contexts*. Trusted contexts also allow security administrators to gain more control over when a privilege or an authority becomes available to a user. For example, a security administrator can use trusted contexts to make sure that a database administrator (DBA) can exercise their role only when they are connecting to the database from a specific IP address.

4.2 – IBM DB2 9 for z/OS

Like DB2 for LUW, the DB2 for z/OS security capabilities can be divided into four broad areas: authentication, authorization, encryption, and auditing. Because for many years z/OS has been designed to run multiple applications simultaneously on the same server, these capabilities are mature, proven technologies.

Authentication is the first security capability encountered when a user attempts to use the DB2 for z/OS product. The user must be identified and authenticated before allowed to use any of the DB2 for z/OS services. DB2 for z/OS uses the z/OS Security Server (RACF or equivalent) for authentication and authorization to access any DB2 subsystem.

Authorization is the next security control encountered. When an application gains access to a subsystem, the user has been authenticated and access to DB2 for z/OS is checked using RACF. DB2 for z/OS then controls access to data through the use of identifiers associated with the authenticated user. A set of one or more DB2 for z/OS identifiers, called authorization IDs, represent the user on every process that connects to or signs on to DB2 for z/OS. These IDs make up the SQL ID. The SQL ID and role, if running in a trusted context, are used for authorization checking within DB2.

Access to DB2 for z/OS requires the use of packages. Packages are required to execute SQL statements. They also have an owner ID or role associated with it. The owner may be different from the SQL ID or role executing the package. To execute any SQL statements bound in a package, the SQL ID or role associated with the package must have the execute privilege on the package. The package owner is used for privilege checking for any static SQL statements in the package. When executing a dynamic SQL statement, the SQL ID or role must be authorized to perform the action against DB2 not the owner. This allows DB2 for z/OS to perform as much authorization checking when the package is created and not every time it is used. Also this approach eliminates the need to authorize all users to all objects used in a package.

Encryption can be employed to keep information confidential when it is transmitted between a DB2 for z/OS subsystem and a DB2 for z/OS client or when it is stored on disk. For data transmission confidentiality, DB2 for z/OS provides two options: native data stream encryption supported in the database protocols and Secure Sockets Layer (SSL) supported in the network layer. The native data stream encryption uses DES to provide a level of performance over SSL. For SSL, DB2 for z/OS exploits z/OS Communications Server's Application Transparent Transport Layer Support (AT-TLS). This facilitates the use of SSL encryption of data during data transmission between DB2 for z/OS systems on behalf of DB2 for z/OS. For data-at-rest encryption, there are also two options: the native encryption and decryption column functions provided by the DB2 for z/OS and the IBM Data

Encryption for IMS and DB2 Databases tool used to encrypt rows. When offloading backups and archive logs, the tape units offer encryption built-in to the drive to protect the archive tape. All exploit System z™ Crypto hardware features to provide better performance and industry level security built-in to z/OS.

The audit facility integrated into z/OS can be turned on to track user actions in DB2. Auditors can collect log and trace data in an audit repository, and then view, analyze, and generate comprehensive reports on the data using the IBM DB2 Audit Management Expert for z/OS. You can selectively filter SELECT, INSERT, UPDATE, and DELETE activity by user or by object, and export these filters for use on another DB2 subsystem.

You can take advantage of mandatory access control in DB2 to protect table data based on the security labels of the rows. When a user accesses a row or a field in the row with an SQL statement, DB2 for z/OS calls RACF to verify that the user is allowed to perform the type of access that is required for the SQL statement. The access is allowed only if the user has the requested access right to all of the rows containing fields that are accessed as part of the SQL statement. For all fields that the SQL statement accesses, DB2 for z/OS checks the security label of the row containing the field and denies access when the user's security label does not dominate the security label of the any one of the rows containing the fields.

A powerful security enhancement in DB2 9 for z/OS is the introduction of trusted contexts, a feature that supplies the ability to establish a connection as trusted when connecting from a certain location or job. Having established a trusted connection, it provides the possibility of switching to other user IDs, thus giving the opportunity of taking on the identity of the user associated with the SQL statement. In addition, it is possible to assign a role to a user of a trusted context. The role can be granted privileges and can therefore represent a role within the organization in the sense that it can hold the sum of privileges needed to perform a certain job, application, or role. These two constructs together supply security enhancements for a variety of different scenarios ranging from any three-tier layered application such as SAP to the daily duties of a DBA maintaining the DB2 for z/OS subsystem.

4.3 – IBM Informix Dynamic Server 11

Similar to DB2, the security capabilities of the Informix Dynamic Server 11 software (“IDS”) can be split into the four areas of authentication, authorization, encryption, and auditing.

Before a user is permitted to connect to an IDS database, the system authenticates them. You can configure the way that IDS authenticates users. The primary authentication mechanism is based on the operating system identity of the user. However, you can configure IDS to use PAM (Pluggable Authentication Modules) to authenticate users using other systems such as LDAP.

Once authenticated, a user will still be denied access unless they are also authorized to perform the intended action. This includes permission to access a particular database, as well as separate controls for each object in the database.

IDS supports encryption in a number of ways. For the Informix client applications using the SQLI protocol, you can configure the communications between the client and server so that all communications between them are encrypted using the ENCCSM module, or you can encrypt the password using the SPWDCSM. If you are using DRDA clients, you can configure them to use SSL. To enhance the secrecy of data in the database, you can use column-level encryption to encrypt particular values. Alternatively, you can use IBM Database Encryption Expert to help secure the disks on which your data is stored. Depending on the backup system you use, you can encrypt the backup data.

The auditing facilities in IDS permit you to track who did what to the data in the system and when they did it. You can control which users and which actions are audited.

IDS also supports mandatory access control through LBAC. This LBAC implementation is very similar to the version for DB2 for LUW. You can apply labels to columns and rows, and grant labels to users, and the system determines whether the user is permitted to see or modify the data.

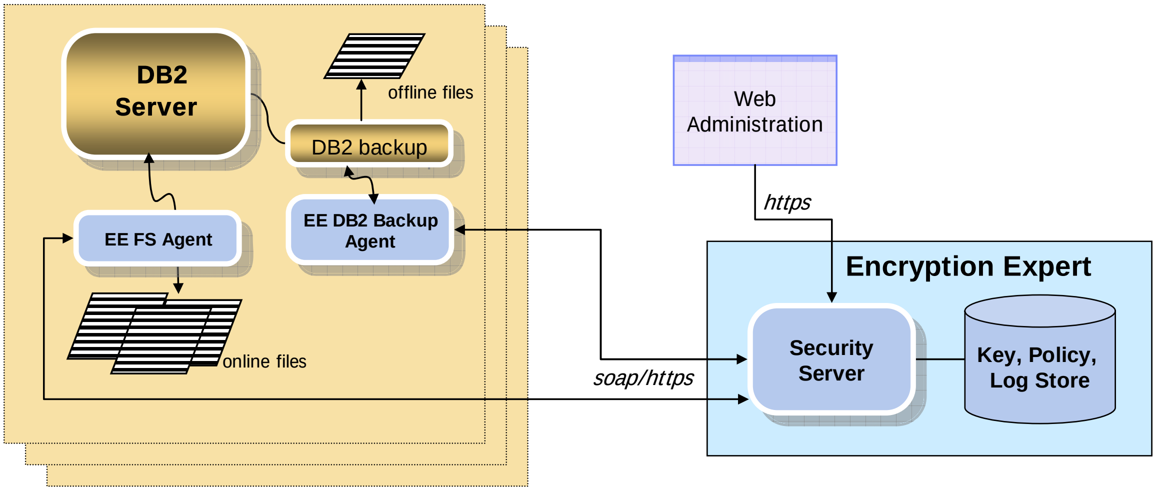
4.4 – IBM Database Encryption Expert 1.1.1

The IBM Database Encryption Expert 1.1.1 software ("IBM Database Encryption Expert") is a data access control tool that combines file encryption with host-level access controls and operational controls. It provides the means, through centrally managed policy, to control the "who, what, when, where, and how" data is accessed on the files on the operating system. These controls can be applied to the database applications, database containers, and other elements in the operating environment.

IBM Database Encryption Expert is a two-component solution composed of one or more software Security Servers and Data Security Agents. This architecture provides separation of duties so the database administrator does not have the same data security privileges as the Database Encryption Expert administrator. The Security Server acts as the centralized point of administration for encryption key, data security policy, and audit log collection.

IBM Database Encryption Expert currently has two agents:

- **Online Data Protection Agent** provides encryption services and access controls for data in online storage accessed by file systems.
- **Secure Backup Agent** provides encryption services for data being backed up to offline storage – both disk and tape.



An important distinction between IBM Database Encryption Expert and other solutions that offer encryption is how the encryption is performed. IBM Database Encryption Expert employs a technique in which the file metadata is left in clear text (unencrypted) while the file contents are encrypted. This technique provides an additional level of file access control in addition to what the file system offers – access without viewability. Effectively, an application can be granted access to a file for the purposes of management without decrypting its contents. Privileged super users can continue to manage their environments and access the file but be restricted from having clear-text access to the file content. This capability helps mitigate risks from internal malicious activity targeted at private/confidential data.

IBM Database Encryption Expert Security Policy Overview

Security policies are at the core of IBM Database Encryption Expert.

They control the following aspects of data security:

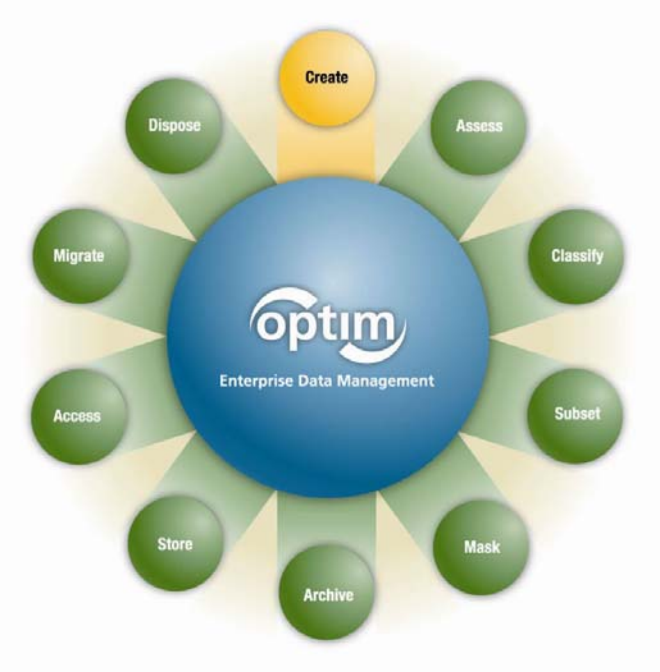
- Who and what can access data
- When data can be accessed
- Where data can be accessed from
- How data is accessed

Policies also control the use of encryption keys and what events are logged (for example, all file accesses, policy violations, and so on). These data security policies allow organizations to translate business rules into data access control and protection policies.

The policy engine is managed through a browser interface hosted from the Security Server. From one Security Server, the policies for many database servers and Database Encryption Expert agents can be managed. Geographical proximity is not a restriction as long as there is IP connectivity between the IBM Database Encryption Expert agents that reside on a DB2 for LUW database servers and the Security Server. It is possible (in fact, it is a best practice) to cluster the Security Servers for high availability and failover.

4.5 – IBM Optim

IBM Optim software is a single, scalable, interoperable Information Lifecycle Management solution providing a central point to deploy policies to extract, store, port, and protect application data from creation through to deletion.



IBM Optim can provide the following core functionality:

Test Data Management: IBM Optim assists in application deployment by streamlining the way you create and manage test environments. Subset and migrate data to build realistic and right-sized test databases. Eliminate the expense and effort of maintaining multiple database clones.

Data Privacy: Protecting your sensitive data does not stop at your production system. This data is commonly replicated in multiple test environments across your organization, as well as in extract files and staging tables. IBM Optim provides automatic data transformation capabilities to mask personal information and de-identify confidential information to protect privacy. You can then use the transformed data safely for application testing, which helps you address compliance requirements and maintain client loyalty.

Archive: IBM Optim provides proven database archiving capabilities, empowering organizations to segregate historical from current data, and to store it securely and cost-effectively while maintaining universal access to the data, thus allowing your production databases to serve your business applications at higher performance levels.

4.6 – IBM DB2 Audit Management Expert 1.1

IBM DB2 Audit Management Expert 1.1 software (“IBM DB2 Audit Management Expert”) is a tool that gives auditors, security administrators, and database administrators (DBAs) the capabilities they need to deliver accurate, timely data and reports for use in auditing activities. It collects the audit records generated from the DB2 audit facility for your DB2 data servers in one audit repository, and allows the auditor to easily view, analyze, and generate reports from these audit records.

From this one centralized tool, auditors can:

- Selectively audit all inserts, updates, deletes, and reads in DB2 databases using automatic processes.
- View all reported activity on specific DB2 objects.
- Generate meaningful reports on the data collected in the audit repository.

IBM DB2 Audit Management Expert separates the roles of auditor and DBA, freeing up the valuable DBA resources used to support auditing requests today. Auditors are not required to be privileged users on the systems they are auditing so database security is preserved. Where a significant auditing exposure is suspected, DB2 Audit Management Expert allows an authorized auditor to investigate the exposure by reviewing what data has been changed in the system. This enables auditors to do database auditing work without DBA involvement. And in a similar fashion, DBAs and security administrators can use the tool to ensure their system is audit-ready.

With the benefit of an easy-to-use graphical user interface, auditors can customize data collection capabilities, defining filter policies based on any combination of DB2 objects, DB2 user IDs, applications connecting to DB2, and time of collection.

DB2 Audit Management Expert also provides a reporting interface that facilitates common auditing tasks such as determining who updated a particular object in a certain timeframe, or monitoring unauthorized access for specific systems or objects. Robust reporting options enable auditors to view and report on data from several perspectives.

Lastly, a separate user-friendly administration interface enables DB2 Audit Management Expert administrators to easily define DB2 Audit Management Expert entities such as collection criteria, users and groups. The interface simplifies administrative tasks with easy-to-use wizards to guide the administrator through each task.

4.7 – z/OS Security Server: Resource Access Control Facility

The Resource Access Control Facility (RACF) software is a component of z/OS System Authorization Facility (SAF), used to protect all resources on z/OS including your network and communications. SAF is the high-level infrastructure that allows you to plug into any commercially available security product.

RACF has evolved over more than 30 years to provide protection for a variety of resources, features, facilities, programs, and commands on the z/OS platform. The RACF concept is very simple: it keeps a record of all the resources that it protects in the RACF database. It can, for example, set permissions for file patterns even for files that do not yet exist. Those permissions are then used should the file (or other object) be created at a later time. In other words, RACF establishes security policies rather than just permission records. The RACF initially identifies and authenticates users by user ID and password when they log on to the system. When a user tries to access a resource, RACF checks its database and, based on the information that it finds in the database, it either allows or denies the access request.

4.8 – z/OS Communications Server: Application Transparent Transport Layer Security

The Transport Layer Security software, or TLS, is the latest evolution of Secure Sockets Layer (SSL) technology. With it, you can encrypt and protect your most important e-commerce transactions and other data transmissions as they cross the network. Implementing and taking advantage of this highly secure approach used to require extensive programming changes to applications within the mainframe environment. With the availability of Application Transparent Transport Layer Security (AT-TLS), you can now deploy TLS encryption without the time and expense of re-coding your applications.

AT-TLS support is policy driven and is managed by a Policy Agent or PAGENT. Socket applications continue to send and receive clear text over the socket, but data sent over the network is protected by system SSL. Support is provided for applications that require awareness of AT-TLS for status or to control the negotiation of security.

CHAPTER 5: SUMMARY

Threats to sensitive and confidential data are multi-faceted and constantly evolving. Protecting your data servers against these broad-based threats requires you to first itemize and understand the threats themselves, and then put in place effective countermeasures to address every threat that is relevant in your environment. This is no trivial task – but the central importance of data security to our society today makes it a job that cannot be ignored or taken lightly.

The most important of these countermeasures involves building security-oriented business practices, processes and controls into your environment. For example, the practice of separation of duties and the principle of least privilege are fundamental security practices that must be present in any security-conscious environment.

But it does not stop at these controls and practices. Utilizing the proper technology, in the proper way, is a critical part of the solution. This begins by first making sure you are using a secure enterprise data server, such as IBM DB2 and IBM IDS. Both data servers feature extensive security and auditing capabilities to help protect sensitive data living in the data server. Secondly, these servers can be enhanced by utilizing critical security-enhancing tools such as IBM Database Encryption Expert, IBM Optim, DB2 Audit Management Expert, and z/OS RACF – providing important layers of security critical to hardening your environment.

In this paper, we introduced and explained the IBM Data Server Security Blueprint. This document enumerates the most common data security threats and outlines effective, proposed countermeasures to each of these threats for users of IBM DB2 and IBM IDS data servers. IBM personnel, armed with the IBM Data Server Security Blueprint and deep security knowledge, can help provide you with a comprehensive look at the threats aimed at sensitive and confidential data today and advise you how best to protect your systems against those threats.

In addition, a collection of important security-related references and documents are provided in Chapter 6 for readers to get more information about each of the recommended countermeasures and associated products.

IBM DB2 and IBM IDS have long been industry leaders of the “SHARP” characteristics: Scalability, High Availability, Reliability, and Performance. With the increased importance of data server security and the in-depth security capabilities that IBM DB2 and IDS bring to the table – as well as the IBM Data Server Security Blueprint – we add another important characteristic and henceforth update the acronym to **SHARPS**: Scalability, High Availability, Reliability, Performance and **Security**.

MORE INFORMATION

DB2 Security

[1] DB2 Information Center
http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp

[2] DB2 9.5 for LUW - Security Manual
ftp://ftp.software.ibm.com/ps/products/db2/info/vr95/pdf/en_US/db2sece950.pdf

[3] IBM Redbooks® Publication: DB2 Security and Compliance Solutions for Linux, UNIX, and Windows
http://www.redbooks.ibm.com/redbooks.nsf/RedpieceAbstracts/sg247555.html?Open

[4] DB2 Label-Based Access Control, A Practical Guide, Part 1: Understand the basics of LBAC
http://www.ibm.com/developerworks/edu/dm-dw-dm-0605wong-i.html?S_TACT=105AGX11&S_CMP=LIB

[5] DB2 Label-Based Access Control: A Practical Guide, Part 2: A step-by-step guide to protect sensitive data using LBAC
http://www.ibm.com/developerworks/edu/dm-dw-dm-0605wong2-i.html

[6] Document-level security using DB2 9 pureXML and LBAC
http://www.ibm.com/developerworks/edu/dm-dw-dm-0607williams-i.html

[7] DB2 Trusted Contexts: Making Security Compliance Easier, IDUG Solutions Journal, Volume 14, Number 2, Summer 2007

DB2 for z/OS Security

[8] Securing DB2 & MLS z/OS
http://www.redbooks.ibm.com/abstracts/sg246480.html

[9] Introduction to the New Mainframe: z/OS (Security Section)
http://www.redbooks.ibm.com/abstracts/sg246366.html

[10] Introduction to the New Mainframe: Security
http://www.redbooks.ibm.com/abstracts/sg246776.html

[11] Communications Server for z/OS V1R8 TCP/IP Implementation Volume 4: Policy-Based Network Security
http://www.redbooks.ibm.com/abstracts/sg247342.html

[12] Data Encryption for IMS and DB2 Databases User's Guide
http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.imstools.deu.doc.ug/decu1a10.pdf?noframes=true

[13] Introduction to RACF: z/OS Version 1 Release 8 RACF Implementation
http://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/sg247248.html?Open

Informix Security

[14] Informix Security Guide: IBM Informix Dynamic Server v11 Information Center.
http://publib.boulder.ibm.com/infocenter/idshelp/v111/index.jsp

[15] Security and Compliance Solutions for IBM Informix Dynamic Server
http://www.redbooks.ibm.com/redbooks.nsf/RedpieceAbstracts/sg247556.html?Open

[16] Enhance Informix Dynamic Server Security Using the Pluggable Authentication Module Framework and JDBC
http://www.ibm.com/developerworks/db2/library/techarticle/dm-0704anbalagan/

[17] Using the PAM Authentication Method with ESQL/C
http://www.ibm.com/developerworks/db2/zones/informix/library/techarticle/0306mathur/0306mathur.html

Information Management Data Governance Tools

[18] IBM Data Governance Web site
http://www.ibm.com/software/data/db2imstools/solutions/compliance.html

[19] IBM Database Encryption Expert: Securing data in DB2
ftp://ftp.software.ibm.com/software/data/db2imstools/whitepapers/IMW14003-USEN-01.pdf

[20] Employing IBM Database Encryption Expert to meet encryption and access control requirements for the Payment Card Industry Data Security Standards (PCI DSS)
ftp://ftp.software.ibm.com/software/data/db2imstools/whitepapers/IMW14002-USEN-01.pdf

[21] IBM Optim Data Privacy
http://www.optimsolution.com/Solutions/DataPrivacy.asp

[22] IBM Database Encryption Expert Web site
http://www.ibm.com/software/data/db2imstools/database-encryption-expert/

[23] IBM DB2 Audit Management Expert Web site
http://www.ibm.com/software/data/db2imstools/db2tools/db2ame/

[24] IBM DB2 Audit Management Expert for z/OS User's Guide, Version 2 Release 1
http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2tools.adh.doc.ug/adhugb20.pdf?noframes=true

[25] IBM Tools – All Product Manuals
http://www.ibm.com/software/data/db2imstools/db2tools-library.html#auditxpertmp-lib

ACKNOWLEDGMENTS

Key Contributors: Jonathan Leffler, James Pickel, Gord Davison
Key Reviewers: Curt Cotner, Tim Vincent, Paul Bird, Paul Zikopoulos, Dwaine Snow, Danny Arnold, Chris Eaton, Bob Harbus, Fred Booker
General: Bruce Johnson, Kevin Street

IBM Canada
8200 Warden Avenue
Markham, ON
L6G 1C7
Canada

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. The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those 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.

The information in this white paper is provided AS IS without warranty. Such information was obtained from publicly available sources, is current as of 03/02/2008, and is subject to change. Any performance data included in the paper was obtained in the specific operating environment and is provided as an illustration. Performance in other operating environments may vary. More specific information about the capabilities of products described should be obtained from the suppliers of those products.