

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

DB2 Version 9.1.1

Report Number: CCEVS-VR-07-0005

Dated: 26 January 2007

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

| | | |
|----|--|----|
| 1 | EXECUTIVE SUMMARY | 3 |
| 2 | IDENTIFICATION | 4 |
| 3 | SECURITY POLICY | 5 |
| | 3.1 IDENTIFICATION AND AUTHENTICATION | 5 |
| | 3.2 USER DATA PROTECTION | 5 |
| | 3.3 AUDIT | 5 |
| | 3.4 TSF PROTECTION..... | 5 |
| | 3.5 SECURITY MANAGEMENT | 5 |
| 4 | ASSUMPTIONS & CLARIFICATION OF SCOPE | 6 |
| | 4.1 USAGE ASSUMPTIONS | 6 |
| | 4.2 CLARIFICATION OF SCOPE | 7 |
| 5 | ARCHITECTURAL INFORMATION | 8 |
| 6 | DOCUMENTATION..... | 11 |
| 7 | IT PRODUCT TESTING..... | 11 |
| | 7.1 VENDOR TESTING | 11 |
| | 7.2 EVALUATOR TESTING | 12 |
| 8 | EVALUATED CONFIGURATION..... | 14 |
| 9 | RESULTS OF THE EVALUATION..... | 14 |
| 10 | VALIDATOR COMMENTS AND RECOMMENDATIONS | 17 |
| 11 | SECURITY TARGET..... | 17 |
| 12 | GLOSSARY | 18 |
| 13 | BIBLIOGRAPHY | 19 |

1 EXECUTIVE SUMMARY

This report documents the NIAP validator's assessment of the CCEVS evaluation of the IBM Corporation DB2 Version 9.1.1. The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory and was completed during December 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the validator. The evaluation determined that the product conforms to the Common Criteria Version 2.3, Part 2 extended and Part 3 and meets the requirements of EAL 4 augmented with ALC_FLR.1 (Basic Flaw Remediation).

The TOE is an IBM Corporation relational database management system. The TOE provides interfaces to clients connected to the database server. From the client, commands can be entered interactively or through an executing program to the database server to create databases, database tables, and to store and retrieve information from tables. The TOE operates as a set of software applications in an IT environment consisting of the hosting operating system and platform (not included in the evaluation). The security services of the IT environment required by the DB2 TOE have not been evaluated and therefore, need to be determined and assessed separately. These IT security services provided by the environment include protection of the TOE security Functions (TSF) domain separation (preventing bypass of the security functions), reliable time-stamps (used in time-stamping audit records), audit generation, security management and user identification and authentication.

The DB2 TOE provides functionality to meet security requirements in the areas of: security audit (generation, association of users in events, and audit review), user data protection, (implementation of a discretionary access control policy (DAC) and a label based access control (LBAC) policy for its objects), identification and authentication, security management and protection of the TSF (enforcement of the security policy). The TOE environment and the TOE security requirements are stated in the DB2 9.1.1 Security Target, Version 1.0, 23 January 2007.

The TOE includes DB2 Enterprise Server Edition Versions for Linux, Unix and Windows operating systems.

The validator observed the activities of the evaluation team, participated in a team meeting, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validator's observations support the conclusion that the product satisfies the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validator concludes that the findings of the evaluation team are accurate, and the conclusions justified.

2 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List. Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if applicable);
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

| Item | Identifier |
|-----------------------------|---|
| Evaluation Scheme | United States NIAP Common Criteria Evaluation and Validation Scheme |
| Target of Evaluation | IBM DB2 Enterprise Server Edition V9.1.1 for Linux, Unix, and Windows |
| Protection Profile | None |
| Security Target | IBM DB2 Enterprise Server Edition V9.1.1 for Linux, Unix, and Windows Security Target, Version 1.0, 23 January 2007 |
| Evaluation Technical Report | Final Evaluation Technical Report For IBM DB2 Version 9.1.1, 12/18/06 |
| CC Version | Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005. Part 2: Security functional requirements, Version 2.3, August 2005 Part 3: Security assurance requirements, Version 2.3, August 2005. |
| Conformance Result | Part 2 extended, Part 3 conformant, EAL4 augmented |
| Sponsor | IBM Canada, Ltd. |
| Developer | IBM Canada, Ltd. |
| Evaluators | SAIC, Columbia, MD |
| Validators | Stephen Butterfield, MitreTek Systems |

3 SECURITY POLICY

The TOE implements the following Security Policies.

3.1 Identification and Authentication

The TOE implements an Identification and Authentication policy which is responsible for ensuring that no database operations can be performed until the DB2 Instance can confirm (using support of the operating system) that the identified user is identified and authenticated and maintaining the association of user security attributes with subsequent operations once an authenticated connection is established.

3.2 User Data Protection

The TOE implements a discretionary access control, residual information protection, and rollback policy. The TOE provides User Data Protection in the following ways:

- Making and enforcing the access decisions for databases and their associated objects that are subject to the discretionary access control policy and the label based access control policy.
- Ensuring that protected objects do not contain residual information when they are created, and,
- Providing the ability to roll back operations on database objects and their content.

3.3 Audit

The TOE enforces the generation of audit records according to how it is configured (e.g. based upon audit type), including the timestamp from the operating system in the audit records, and provides support for the review of the audit data.

3.4 TSF Protection

The TOE provides support for the Protection of the TSF security function at its interfaces by allowing access only when its security mechanisms have been successfully invoked. Additionally, the TOE collects time information from the environment (i.e., the operating system)

3.5 Security Management

The TOE provides security management functionality necessary to manage TOE data. The functionality includes support for the following:

- Management of the audit function and review of audit data, allowing access to functions that manage user security attributes (granting and revoking), and;

- Management of access control settings on databases content.

The TOE supports the roles of authorized administrator and user. As part of the security management policy, the TOE also ensures that only authorized administrators can perform functions not allowed to normal users.

4 ASSUMPTIONS & CLARIFICATION OF SCOPE

4.1 Usage Assumptions

The system is expected to be used in what has traditionally been known as a relatively benign, or non-hostile, environment.

The Assumptions as presented in the ST are noted below.

Personnel Assumptions

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
- Procedures exist for granting users authorization for access to specific security levels.

Physical Assumptions

The TOE is intended for application in areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Connectivity Assumptions

- All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.
- The IT Environment underlying the TOE is assumed to fulfill the requirements for the IT Environment described in this ST. It is also assumed that the IT Environment will

provide a suitable operational environment for the TOE where the TOE will be able to properly execute and the dependencies that the TOE has upon the IT Environment are properly fulfilled.

The ST identifies the following requirements for the IT Environment:

| Security Functional Class | Security Functional Components |
|---|--|
| Security Audit (FAU) | FAU_GEN.1b Audit data generation |
| | FAU_STG.1: Guarantees of Audit Data Availability |
| User Data Protection (FDP) | FDP_RIP.2b Full residual information protection |
| Identification and authentication (FIA) | FIA_ATD.1b User attribute definition |
| | FIA_SOS.1 Verification of secrets |
| | FIA_UAU.2b User authentication before any action |
| | FIA_UAU.7 Protected authentication feedback |
| | FIA_UID.2b User identification before any action |
| Security management (FMT) | FMT_MTD.1c Management of TSF data |
| | FMT_MTD.1d Management of TSF data |
| | FMT_MTD.1e Management of TSF data |
| | FMT_REV.1b Revocation |
| | FMT_SMF.1b Specification of Management Functions |
| | FMT_SMR.1b Security Management Roles |
| Protection of the TSF (FPT) | FPT_AMT.1 Abstract Machine Testing |
| | FPT_RVM.1b Reference Mediation |
| | FPT_SEP.1 Domain Separation |
| | FPT_STM.1b Reliable Time Stamps |

4.2 CLARIFICATION OF SCOPE

The Security Target delineates the security requirements of the TOE, which determined the scope of the evaluation. The security requirements allocated to the IT environment have not been verified as part of the DB2 TOE evaluation. The IT security services provided by the environment support the protection of the TOE security Functions (TSF) including domain separation, reference mediation (preventing bypass of the security functions), reliable time-stamps (used in time-stamping audit records), audit generation, security management and user identification and authentication. The FPT_SEP.1 requirement is allocated exclusively to the IT environment. Therefore, the scope of the evaluation does not include a determination of the ability of the TOE to protect itself from tampering or the ability to maintain a security domain that is protected from interference and tampering by untrusted subjects or to enforce separation between the security domains of subjects in the TOE Scope of control. Other SFRs allocated

exclusively to the IT environment include FIA_SOS.1, FIA_UAU.7 and FPT_AMT.1. Therefore the IT environment is also exclusively responsible for meeting the strength metrics for authentication secrets, obscuring feedback during authentication, and providing abstract machine testing.

5 ARCHITECTURAL INFORMATION

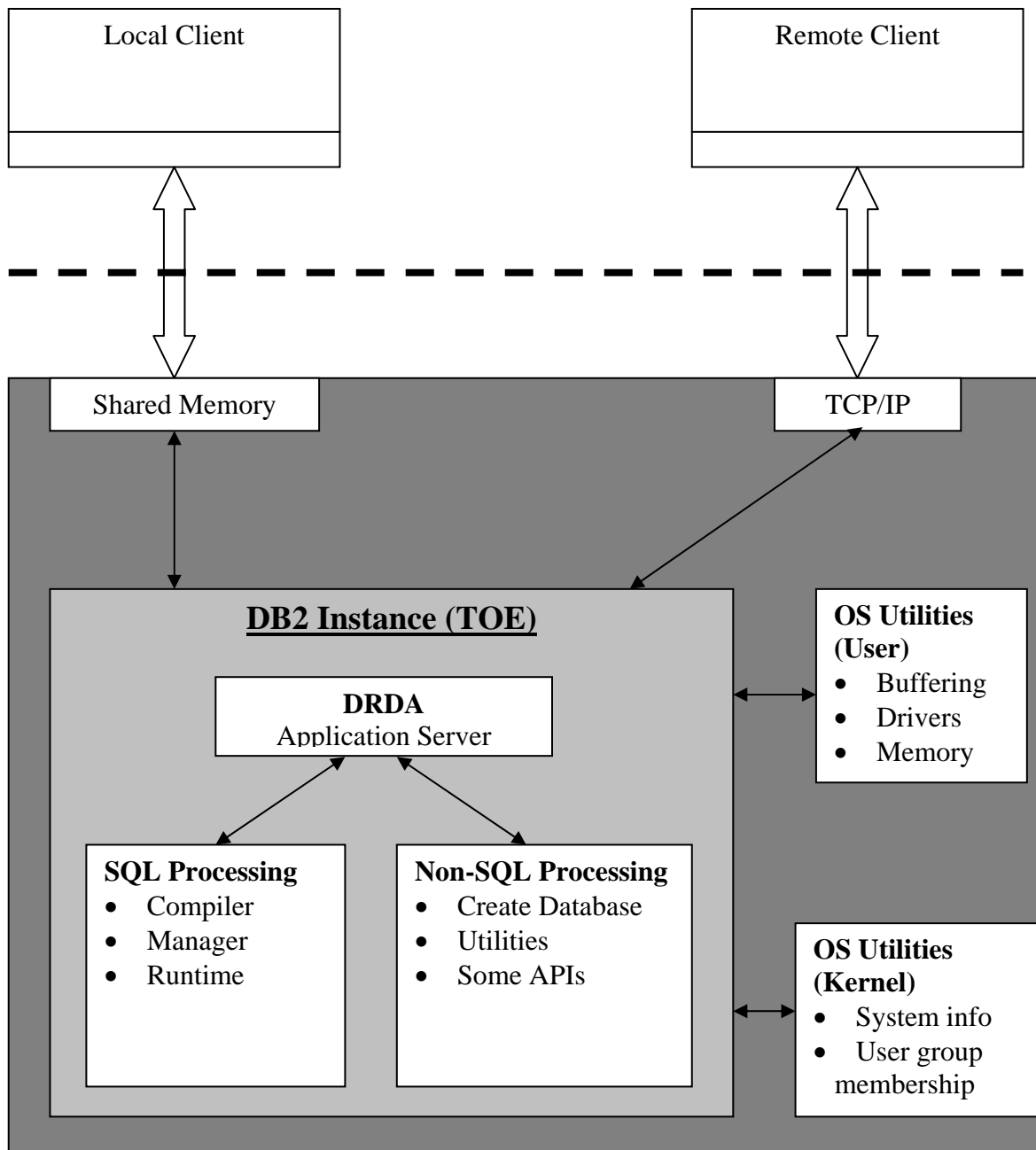
DB2 is a relational database management system (RDBMS) provided by IBM. As a RDBMS, DB2 supports the Standard Query Language (SQL) interface from a client that is connected to the database server. From the client, commands can be entered interactively or through an executing program to the database server to create databases, database tables, and to store and retrieve information from tables. DB2 can be installed on a number of possible operating environments.

DB2 operates as a set of applications (e.g., servers and command line programs) in an IT Environment including a hosting operating system and platform. The IT Environment provides fundamental supporting mechanisms to DB2. In particular, it supplies a trusted authentication mechanism and utilities to manage system resources.

DB2 is realized as a running server (i.e., DB2 Instance) and a set of commands (i.e., DB2 Commands) that can be exercised by appropriate users. The TOE is described in terms of two subsystems – the Security Management subsystem and the Server subsystem.

The Security Management subsystem is responsible to provide the tools and server interfaces necessary for administrators and other users to manage the security-relevant configuration of DB2. Note that the Security Management subsystem implements only some of the security management related functions, however it is so named because it provides all of the interfaces that are to be used for security management. In the cases where the security management functions are implemented, entirely or in part, in the Server subsystem, the Security Management subsystem provides the user interface and interacts with the Server subsystem to affect the function. The Server subsystem is responsible to implement database instances, offering interfaces for the creation and manipulation of databases and associated database objects.

The TOE for the DB2 configuration includes all components within the lightly shaded box entitled “DB2 Instance”. For the purposes of this ST, the TOE is at least one partition, but can be distributed across a number of logically (i.e., on the same underlying machine) or physically (i.e., on different underlying machines) separate partitions. This latter feature is known as Database Partitioning Feature (DPF). From the user perspective, there is effectively no difference, while the distributed partitions work in concert to answer user queries. In relation to the figure above, the ‘DB2 Instance’ may actually be distributed across multiple DB2 partitions acting together to form that logical view.



All other functions are allocated to the IT Environment, which in this case is the Host Operating System (OS), inside the darkly shaded box. The DB2 software is tightly linked to the OS and in some cases, security functions are allocated to the OS, as appropriate. For the purposes of this ST, the OS is AIX 5.3 , Linux RHEL 4, Linux SLES 9 with SP2, Microsoft Windows Server 2003 Enterprise Edition with SP1, or Solaris 9.

This section describes the basic functions performed within DB2. These functions are depicted as

individual blocks within the DB2 Instance (TOE) box in the figure above. DB2 is implemented using the concept of a DB2 instance where an instance is a complete environment dictating what can be done to data and managing the system resources assigned to it. A DB2 instance has one or more databases under its control that cannot be directly accessed by any other instance.

DB2 implements a Discretionary Access Control (DAC) security policy by default and a label based access control (LBAC) policy when configured. This permits a confidential security mechanism to ensure data is protected against unauthorized or accidental disclosure or destruction. Auditing is supported at the DB2 instance level meaning that all modules within the TOE are capable of creating audit events. Review and analysis of the audit logs is restricted to users with system administrator authority.

DRDA Protocol Handler

The DRDA Application Server (AS) module within DB2 allows for DB2 to act as an Application Server within the Distributed Relational Database Architecture (DRDA). DRDA is an OpenGroup standard used in the management of distributed data. The DB2 DRDA AS module architecture provides support for one or more DRDA Application Requestors (DRDA AR), commonly referred to as clients, to access a specific DB2 instance or DB2 database and issue SQL and non-SQL requests against that object. Upon initiation of communication between a client and the DB2 DRDA AS module, a common "security mechanism" is negotiated. This mechanism may be one of a number of different security protocols; for the purpose of this TOE, the only allowed security mechanism is the "Userid, Password" mechanism as described in the DRDA standard. If validation of the password fails, the DRDA AS terminates conversation with the client that provided the failed password. If the password is authenticated, a DRDA session, or connection, is established and the client may begin to pass requests to DB2 for processing. These requests are of two general types: SQL requests, which are handled by the DB2 SQL Processing module, and non-SQL requests, which are handled by the DB2 Non-SQL Processing module. The DRDA AS module identifies the type of request and passes it to the appropriate module for further processing.

SQL Processing

The DB2 SQL Processing module is responsible for the analysis and execution of client requests related to the processing of Structured Query Language (SQL) statements. DB2 supports the ANSI/ISO SQL2 standard for all types of SQL statements including:

- Data Definition Language (DDL) statements that create, alter, drop, rename, or transfer ownership of database objects.
- Data Manipulation Language (DML) statements that are used to query or modify the data contained within database objects. Modification can occur in one of three ways: row insertion, row deletion, or row modification via column updates. These statements include SELECT, INSERT, UPDATE, and DELETE SQL statements.
- GRANT and REVOKE statements that are used to control the access to database authorities as well as privileges on database objects
- Transaction control statements that are used to manage the integrity of the database with respect to any modification made by a client. These statements include, among others, the ROLLBACK and COMMIT SQL statements..

- Miscellaneous statements used to perform a number of different actions on database objects or on the connection environment. Such statements would include the LOCK TABLE and SET INTEGRITY statements.

The DB2 SQL Processing module is comprised of three distinct components: the SQL Manager, the SQL Compiler, and the SQL Runtime components.

Non-SQL Processing

The DB2 Non-SQL Processing module is responsible for the analysis and execution of all those client requests not concerned with SQL statements. Such requests are used to invoke a number of Application Program Interfaces (APIs) and utilities provided by DB2 that do not use SQL statements to perform their specified actions. There exist a number of these APIs and utilities at both the DB2 Instance level as well as at the individual database level within a DB2 instance. Each API and utility provided by DB2 has an assigned privilege or authority requirement as defined by DB2. The DB2 Non-SQL Processing module enforces the discretionary access control policy for these non-SQL requests by ensuring that the required privilege or authority is held by either the primary authorization ID, or secondary authorization IDs where applicable, of the requestor.

6 DOCUMENTATION

The developer-issued guidance identified below is based on the documentation provided as evaluation evidence. All documentation provided for the TOE was evaluated.

Guidance documentation

Common Criteria Certification: Installing IBM DB2 Version 9.1 Enterprise Server Edition for Linux, Unix and Windows – Revision 04

Common Criteria Certification: Administration and User Documentation – Revision 02

Security Target

IBM DB2 Enterprise Server Edition Version 9.1.1 for Linux, Unix, and Windows Security Target Version 1.0, 23 January 2007

7 IT PRODUCT TESTING

7.1 Vendor Testing

The description of the vendor suite is documented in the following evaluation evidence documents: Test Cases for the Common Criteria

Testing Approach:

The developer testing approach is described in the Developer Test Plan.

The majority of the testing of the DB2 security functions is performed by a series of automated tests, while a few tests may require some manual steps. These tests can be mapped to the test cases outlined in the Functional Specification document. Together they demonstrate the security-relevant behavior of DB2 at the interfaces defined in that document: the Command Line User Interface, SQL Interface, API Interface, and the DRDA Interface. The goal of the tests is to demonstrate that DB2 meets the security functional requirements specified in the Security Target.

The security functions to be tested are the same as those mentioned in the Security Target: Audit, User Data Protection, Identification & Authentication, Security Management, and Protection of the TSF.

Test Descriptions

The test procedure descriptions are provided in a collection .txt files that include several test cases. For each test case within the .txt file, a description of what is tested (equivalent to a test case in the Functional Specification document) and an overview of how it is tested is provided. A test package is provided for each platform included in the test configuration. The test package includes several directories. Each directory includes the following files, one for each of the .txt test description files:

- .rrn files (test output)
- .sqc (written in C) and .pl (written in perl) files (test source files)
- .rxp files (expected test results files)
- .rrn files (actual test results in the collection of the rrn files)

Depth and Coverage:

The amount of testing performed as it relates to the required functionality is described in the rationale for ATE_COV work units. The depth of testing performed as it relate to the High Level design is described in the rationale for the ATE_DPT work units.

Test Results:

The test suite is an automated test suite with one manual test case. For each test description file (e.g. CC042.txt), there is an .exp file (e.g. CC042.exp) that describes the expected results and a .rrn file (e.g. CC042.rrn) that provides the actual results of a test run. Additional files with the extension .err and .dfr – representing errors and differences, respectively – are also generated detailing any inconsistencies between the .rxp (expected results) file and the .rrn (actual results) file. If no errors are generated during testing, the file with extension .dfr is created with a size of zero (0) bytes and no error file (.err) file is generated.

7.2 Evaluator Testing

The evaluation team performed the TOE installation, as specified in the Installation, Generation and Startup documentation and performed functional, independent and vulnerability testing.

The test configuration consists of Version 9.1 of DB2 installed on two separate machines: one running the Windows 2003 operating system, one running SuSe Linux Enterprise Server 9. The following product options was installed on the following platforms:

Enterprise Server Edition on the Windows 2003 platform:
Optional features: with DPF configured

Enterprise Server Edition on the SuSe Linux Server 9 platform:
Optional features: without DPF configured

The test tools used by the developer test suite are documented in the Developer Test Plan.

The above test configuration were compared to the TOE identification included in the ST and found to be consistent. All platforms included in the ST are included in the vendor test configuration and sufficiently represented in the evaluator test configuration.

The DB2 security testing consisted mainly of automated tests augmented with a few manual procedures. The tests map to the test cases outlined in the IBM Corporation DB2 V9 Universal Database Functional Specification document and demonstrate the security-relevant behavior of DB2 at the interfaces defined in the functional specification. These interfaces consist of the Command Line User Interface, SQL Interface, API Interface, and the DRDA Interface.

The goal of the tests is to demonstrate that DB2 meets the security functional requirements specified in the Security Target. The security functions tested are those described in the Security Target: Audit, User Data Protection, Identification & Authentication, Security Management, and Protection of the TSF. Team tests for audit and access control were performed with passing results. A penetration test for access control (LBAC) was performed with a passing result.

8 EVALUATED CONFIGURATION

IBM DB2 Enterprise Server Edition Version 9.1.1 for Linux, Unix, and Windows (the TOE) is a Relational Database Management System (RDBMS) developed by IBM Canada, Ltd., 3600 Steeles Avenue East, Markham, Ontario L3R 9Z7, Canada and sold by IBM Corporation, Route 100, Somers, NY, USA 10589.

In the evaluation configuration, the TOE can be installed upon

- AIX 5.3
- SuSE Linux Enterprise Server V9
- RedHat Linux (RHEL 4)
- Windows Server 2003 with SP 1
- Solaris 9

9 RESULTS OF THE EVALUATION

The evaluation was conducted based upon CC version 2.3 and CEM version 2.3. The evaluation determined the IBM DB2 TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) requirements augmented with ALC_FLR.1

9.1 Evaluation of the IBM DB2 Security Targets (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the IBM DB2 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

9.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

9.5 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

The evaluation team also applied the ALC_FLR.1 related work units from the Flaw Remediation CEM Supplement (Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R). The evaluation team ensured the developer has a process to track flaws, document flaws, address flaws, and provide flaw information to TOE users.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE security functional requirements are enforced by the TOE. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

9.10 Assurance Requirement Results

The assurance requirements for the TOE evaluation are those required by EAL4.

9.10.1 Common Criteria Assurance Components

The CEM work units associated with EAL4 are distributed amongst the ETR sections in chapter 15 of the ETR. Collectively, the ETR sections in chapter 15 encompass all CEM work units for EAL4. Each ETR section includes the CEM work units associated with that ETR section title (e.g. ACM). Within each ETR section, for each CEM work unit the following is provided:

- Verdict

- Verdict Rationale

The rationale justifies the verdict using the CC, the CEM, and any interpretations and the evaluation evidence examined. The rationale demonstrates how the evaluation evidence meets each aspect of the criteria.

The work performed contains a description of the action performed or the method used to apply the work unit.

9.10.1.1 Testing and Vulnerability Assessment

In addition to ETR sections the evaluator developed a Test Plan/Report Part to capture the detail beyond the CEM work unit information. This detail is described within the CEM guidance for the testing and vulnerability assessment work units. Primarily, the additional detail is focused on team test procedures, penetration test procedures, results from running the vendor's sample, and the justification of running the vendor's sample.

The evaluation team prepared a Draft of the Test Plan/Report prior to testing that addressed the selection of vendor tests to run, the team test procedures, and the penetration test procedures. After performing the test, the Test Report Part was updated to include the actual results from the vendor sample run and the team test.

The Test Report Part is included in chapter 15 of the ETR.

9.11 Conclusions

The conclusions for the ST evaluations and the TOE evaluations are addressed below.

ST Evaluation

Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the IBM DB2 Enterprise Server Edition version 9.1.1 Security Target is a CC compliant ST.

TOE Evaluation

The verdicts for each CEM work unit in the ETR sections included in chapter 15 are each "PASS". Therefore, the IBM DB2 TOE (see below product identification) satisfies the IBM DB2 9.1.1 Security Target, when configured according to the following guidance documentation: Common Criteria Certification: Installing IBM DB2 Version 9.1 Enterprise Server Edition for Linux, Unix and Windows – Revision 04

9.12 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test further demonstrated the claims in the ST.

10 VALIDATOR COMMENTS AND RECOMMENDATIONS

The validator observations support the evaluation team's conclusion that the DB2 9.1.1 meets the claims stated in the Security Target. However, users of the TOE are reminded to be aware of the limitations and cautions contained in Section 4, Assumptions & Clarification of Scope.

11 SECURITY TARGET

The IBM Corporation DB2 Enterprise Server Edition Version 9.1.1 for Linux, Unix, and Windows Security Target, Version 1.0, 23 January 2007 is included here by reference.

12 GLOSSARY

| | |
|-------|--|
| CC | Common Criteria |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCTL | Common Evaluation Testing Laboratory |
| CEM | Common Evaluation Methodology |
| CM | Configuration Management |
| DAC | Discretionary Access Control |
| DDL | Data Definition Language |
| DML | Data Manipulation Language |
| DRDA | Distributed Relational Database Architecture |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| LBAC | Label Based Access Control |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards & Technology |
| NSA | National Security Agency |
| NVLAP | National Voluntary Laboratory Assessment Program |
| OS | Operating System |
| PP | Protection Profile |
| RDBMS | Relational Database Management System |
| SFR | Security Functional Requirement |
| SQL | Structured Query Language |
| ST | Security Target |
| TCSEC | Trusted Computer System Evaluation Criteria |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| TSFI | TOE Security Function Interface |

13 BIBLIOGRAPHY

- [1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.
- [2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3..
- [3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.
- [4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.
- [5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated August 2005, Version 2.3..
- [6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.
- [7] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
- [8] Evaluation Technical Report for IBM DB2 Part 2 (Proprietary), Revision 0.1
- [9] IBM Corporation DB2 9.1.1 Security Target, Version 1.0, 23 January 2007.
- [10] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001