National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Trusted RUBIX™ Version 5.0 Multilevel Security Relational Database Management System

Report Number: CCEVS-VR-04-0079
Dated: October 15, 2004
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

ACKNOWLEDGEMENTS

Validation Team

Brad O'Neill
Yi-Fang Koh
The MITRE Corporation
Bedford, MASSACHUSETTS

Common Criteria Testing Laboratory

COACT
Columbia, Maryland

Evaluation Team

Bob West
Brain Pleffner
Christa Lanzisera
Dawn Adams
Tom Benkart

Table of Contents

Figures

Tables

I. Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of Trusted RUBIX Version 5.0 Multilevel Security (MLS) Relational Database Management System (RDBMS). It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by COACT and was completed on September 30, 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 4, resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE under evaluation is the Trusted RUBIX Version 5.0 Multilevel Security Relational Database Management System for UNIX environments which was designed and manufactured by Infosystems Technology, Inc. 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 (not included in the evaluation) consisting of the hosting operating system and hardware platform.

The Trusted RUBIX TOE was designed for and tested using Sun Microsystems' Trusted Solaris 8 operating system. While Trusted Solaris 8 has been evaluated, not all of the specific security services that are required by the TOE were evaluated and therefore, the IT environment security services need to be determined and assessed separately. The security services provided by the IT environment include reliable time-stamps (used in time-stamping audit records), security management, and user identification and authentication. The TOE and the IT environment work cooperatively to provide the domain separation (preventing bypass of the security functions) and residual data protection security services.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that COACT's findings are accurate, the conclusions justified, and the conformance results correct.

Disclaimers: The information contained in this Validation Report is not an endorsement of Trusted RUBIX Version 5.0 MLS RDBMS by any agency of the U.S. Government

and no warranty of Trusted RUBIX Version 5.0 MLS RDBMS is either expressed or implied.

II. Identification

2.1 TOE, CC, and CEM Identification

TOE: Trusted RUBIX Version 5.0 Multilevel Security Relational Database Management System

Evaluated Software: Trusted RUBIX Version 5.0 Multilevel Security Relational Database Management System

Developer: Infosystems Technology, Inc.

CCTL: COACT

CC Identification: *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999 [CCV2.1].

Interpretations: All NIAP and CCIMB interpretations as of the date of the Kick-off meeting held on October 30, 2002, were considered during the evaluation. The interpretations listed in Table 1 had a direct impact on the work performed.

Table 1. Interpretations impacting the Trusted RUBIX 5.0 evaluation.

Short Title	Subject
National Interpretations	
I-0347	Including Sensitive Information In Audit Records, 2002-08-22
I-0405	American English Is An Acceptable Refinement, 2000-12-20
I-0406	Automated Or Manual Recovery Is Acceptable, 2001-03-15
I-0407	Empty Selections Or Assignments, 2002-01-04
I-0415	User Attributes To Be Bound Should Be Specified, 2002-03-04
I-0416	Association Of Access Control Attributes With Subjects And Objects, 2000-12-05
I-0417	Association Of Information Flow Attributes W/Subjects And Information, 2000-12-11
I-0422	Clarification Of ``Audit Records", 2000-12-05

Short Title	Subject
I-0423	Some Modifications To The Audit Trail Are Authorized, 2000-12-11
I-0427	Identification of Standards, 2001-06-22
I-0429	Selecting One Or More, 2002-01-04
I-0463	Platform Inclusion In A TOE With FPT_SEP
International Interpretations	
RI # 3	Unique identification of configuration items in the configuration list, 2002-02-11
RI # 4	ACM_SCP.*.1C requirements unclear, 2001-11-12
RI #16	Objective for ADO_DEL, 2002-02-11
RI # 31	Obvious vulnerabilities, 2002-10-25
RI #38	Use of 'as a minimum' in C&P elements, 2003-10-31
RI #49	Threats met by the Environment, 2001-02-16
RI #64	Apparent higher standard for explicitly stated requirements, 2001-02-16
RI # 65	No component to call out security function management, 2001-07-31
RI # 69	Informal Security Policy Model, 2001-03-30
RI # 75	Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1, 2000-10-15
RI #84	Aspects of objectives in TOE and environment, 2001-02-16
RI #85	SOF Claims additional to the overall claim, 2002-02-11
RI # 116	Indistinguishable work units for ADO_DEL, 2001-07-31
RI # 127	TSS Work unit not at the right place, 2002-10-25
RI # 128	Coverage of the delivery procedures, 2002-11-15

CEM Identification: *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

2.2 TOE Overview

Trusted RUBIX 5.0 is a multilevel secure Relational Database Management System for the Trusted Solaris UNIX® environment. Trusted RUBIX 5.0 allows different levels of sensitivity data to be represented by different sensitivity labels within a single database. The Mandatory Access Control policy restricts access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity. Trusted RUBIX 5.0 also supports Discretionary Access Control, auditing, and authentication policies.

Trusted RUBIX 5.0 is an SQL-based relational DBMS product operating under an IT environment provided by Trusted Solaris 8 in a standalone or a client/server architecture

as shown in Figure 1. Client processes are untrusted application programs that have been linked with Trusted RUBIX 5.0 client software so that they can communicate with Trusted RUBIX 5.0 server process. There is one instantiation of the server for each active client. A given client and server pair can run on the same machine or on different machines connected via a network. The server process must reside on the same machine as the data to be accessed. Each client is a program that executes with the credentials and privileges of the initiating user. It may reside on the same machine as the server or on a different machine. The Trusted RUBIX 5.0 client component does not perform any security-relevant function. There are two types of clients:

- Interactive Structured Query Language (ISQL) client provides an interactive interface where SQL operations can be typed in or read from a script file.
- Call Level Interface (CLI) is a set of C language function calls that may be used to write application programs to operate on the database.

.

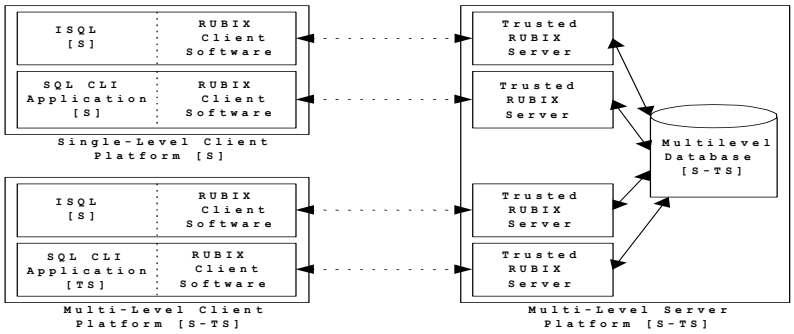

Figure 1. Trusted RUBIX 5.0 Architecture

Evaluated software is Trusted RUBIX 5.0. The Trusted Solaris 8 operating system and hardware upon which the TOE executes were not evaluated, but were assumed to operate correctly and securely.

The overall Strength of Function claim for the TOE is SOF-medium.

III. Security Policy

A high-level description of the Trusted RUBIX 5.0 security policy is as follows.

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Security audit (Audit) functions

- Identification and Subject Binding
- Object reuse
- Secured import and export operations
- Trusted recovery
- Security Management
- Protection of security functions

Details about the TOE security policy is contained in Annex D and within the [ST].

IV. Assumptions and Clarification of Scope

This section provides an overview of the threats and assumptions addressed by the Environment.

4.1 Threats

Detailed description of threats is contained in the Trusted RUBIX 5.0 Security Target. Many of the threats were adapted from threats in the *Multilevel Operating System* protection profile [MOS_MED PP]. The statements of the threats in the security target and the MOS_MED PP are not identical because of differences between a DBMS and an operating system.

4.2 Environmental assumptions

- Database administrators, database operators, DBMS security administrators, and DBMS audit administrators are competent, and merit trust place in them.
- Authorized DBMS users are familiar with applicable DBMS security policies and procedures, and merit the trust placed in them.
- The DBMS is protected against disasters such as loss of power, fire, flood, and destruction of facilities.
- The DBMS, host OS, and IT environment are protected from physical attack.
- The environment protects information while it is in transit between the DBMS and components of the IT environment.
- The operating system which the TOE executes on is assumed to operate correctly and securely.

Additional details about the environment assumptions are contained within Annex E of this Validation Report, and within the [ST]

V. Evaluated Configuration

Details about the evaluated configuration are contained within the Installation and Generation documents identified in Table 2.

Table 2. Installation and generation documents.

Installation and Generation
Trusted RUBIX 5.0 Trusted Facility Manual, Version 1.5.1, January 15, 2004
Trusted RUBIX 5.0 Delivery and Operation, Version 1.4, September 26, 2004

VI. Evaluation Process and Conclusions

The COACT CCTL Evaluation Team followed the procedures outlined in CCEVS Scheme Publication #4, *Guidance to Common Criteria Testing Laboratories* [CCEVS4].

The Evaluation Team concluded that the TOE was found to be CC Part 2 extended and CC Part 3 conformant, and recommended that an EAL4 certificate rating be issued for the TOE.

VII. Validation Process and Conclusions

The Validation Team followed the procedures outlined in CCEVS Scheme Publication #3, *Guidance to Validators of IT Security Evaluations* [CCEVS3].

The Validation Team agreed with the conclusion of COACT Evaluation Team, and recommended to CCEVS Management that an EAL4 certificate rating be issued for the Infosystems Technology Trusted RUBIX Version 5.0 Multilevel Security Relational Database Management System.

VIII. Validator Comments/Recommendations

The evaluator's vulnerability analysis could not reliably determine the attack potential associated with unpatched vulnerabilities in the underlying Trusted Solaris operating system. The evaluated version of Trusted Solaris was assumed for the Trusted RUBIX evaluation. Post-evaluation patches to Trusted Solaris were not considered well-known because the patch information is limited to registered Trusted Solaris customers and is not publicly available. Patches to the Solaris operating system upon which Trusted Solaris was based are publicly available and vulnerabilities corrected by these patches might also exist in Trusted Solaris. The analysis effort to determine if well-known Solaris vulnerabilities would also apply to Trusted RUBIX was beyond the scope of this evaluation and this class of vulnerabilities was not considered exploitable by attackers possessing low attack potential.

The ST derived many of its threats, organizational security policies, and security objectives from the Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness [MOSMPP]. In most cases, the wording was altered to reduce their scope so as to be more appropriate for the functions that were under control of Trusted RUBIX versus the underlying Trusted Solaris operating system. The ST does not contain any protection profile compliance claims and the scope of this evaluation was limited to the specific threats, organizational security policies, and security objectives enumerated in the ST. Furthermore, the version of Trusted Solaris upon which Trusted RUBIX relies was evaluated for compliance against the earlier Labeled Security Protection Profile [LSPP] instead of the [MOSMPP]. While Trusted RUBIX appears designed to satisfy the basic intent of the [MOSMPP], full compliance with the [MOSMPP] should not be assumed.

IX. Annexes

Annex A: Architectural Description of the TOE

Refer to Section 2.2, TOE Overview, and to the Security Target (ST) [ST] for the architectural description.

Figure 2 shows the client/server architecture for Trusted RUBIX 5.0. Each CLI or ISQL client is initiated by a Trusted Solaris 8 user. The client process is unprivileged, running with the user's credentials. When the client process connects to a specific database it will create a Trusted RUBIX 5.0 server process. The server process is started with an *exec* system call for local database and with the *inetd* services for remote databases. The server process sets its user credentials and sensitivity label and then performs operations on behalf of the client. This procedure is performed by the Client/Server Communication Module. The Trusted RUBIX 5.0 Server interacts with the physical data through Trusted Solaris 8 operating system files.

The Client Subsystem's CLI and ISQL Modules provide an interface for the user to interact with the Trusted RUBIX 5.0 Server. These modules communicate with the Trusted RUBIX 5.0 Server through the Trusted RUBIX 5.0 Server Interface Module. The Trusted RUBIX 5.0 Server generally interacts with the physical data using the Common Server Subsystem's Volume Manager.

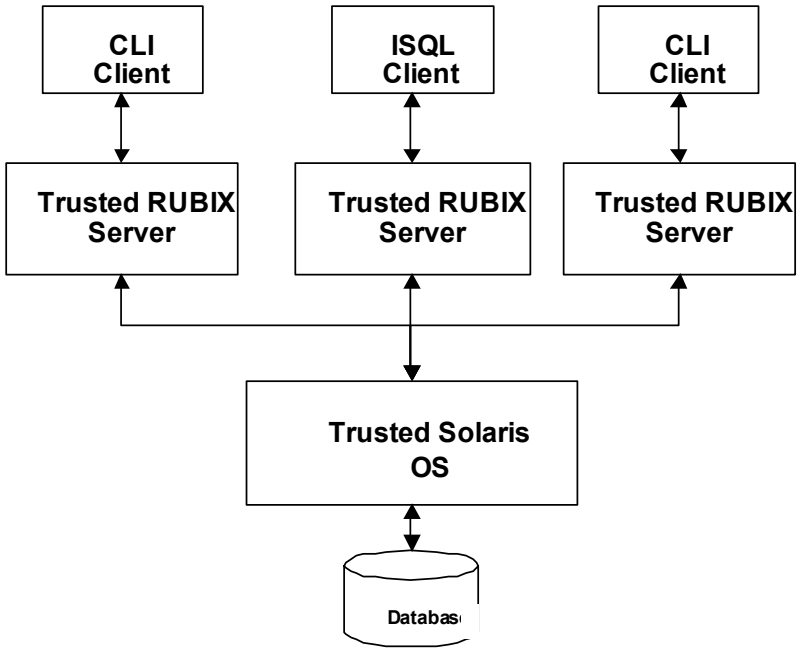

Figure 2. Trusted RUBIX 5.0 Client Server Architecture

Figur 3 shows the major subsystems of the Trusted RUBIX 5.0 server.

- The Client Subsystem accepts SQL operations from the user and sends them from the client process to the server process using a remote procedure call (RPC) interface.
- The Server Interface Subsystem supports the RPC interface and is used to connect and disconnect to specific databases, start and terminate transactions, manipulate savepoints, and execute SQL operations. This subsystem parses the SQL command text into the query tree, optimizes them for performance, and translates the SQL operations into an internally executable form.
- The SQL Engine Subsystem is responsible for enforcing the DAC policy and translates the high level SQL operations into operations on record oriented files.
- The Kernel Subsystem is responsible for enforcing all MAC restrictions on data objects. This subsystem also provides low-level transaction and database operations.
- The Common Server Subsystem encapsulates all modules that require shared data objects in main memory (i.e., buffer management).
- The Common Libraries Subsystem consists of general routines that may be used by any module. Examples include manipulating records and allocating memory.

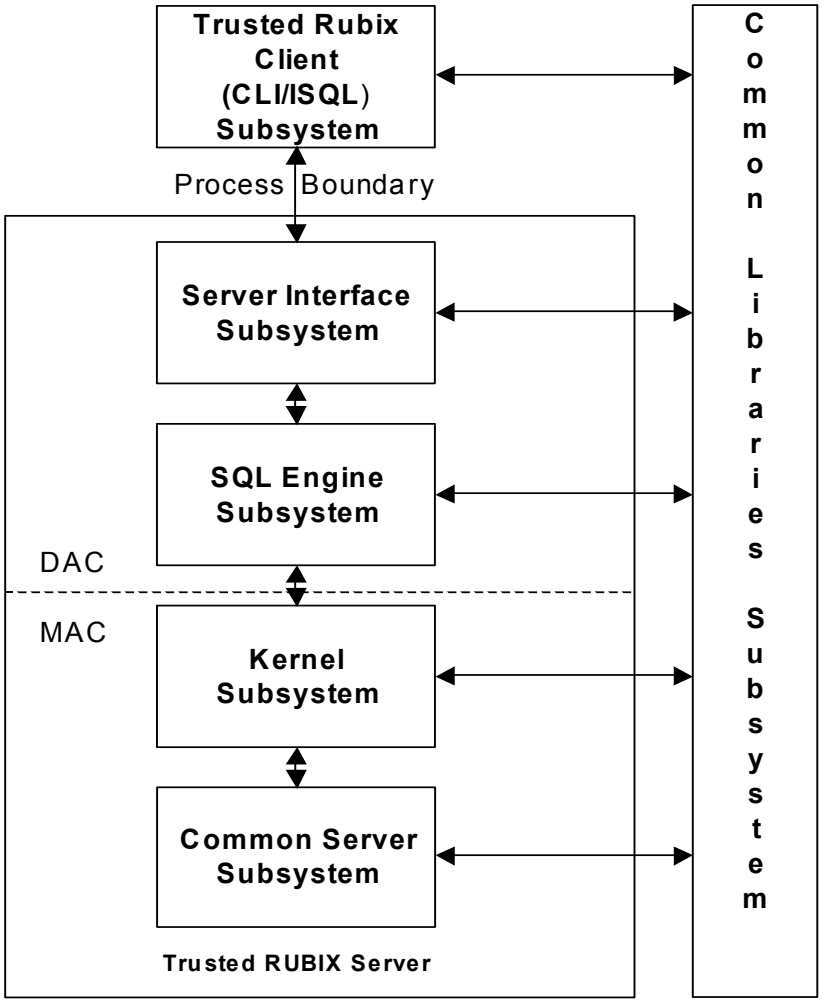

Figure 3. Trusted RUBIX 5.0 High Level Architecture

Annex B: Assurance Requirements Results

Infosystems Technology, Inc. Trusted RUBIX 5.0 MLS RDBMS satisfies the EAL4 security assurance requirements identified in Part 3 of the *Common Criteria* [CCV2.1]. These requirements are displayed in Table 3.

Table 3. TOE security assurance requirements.

Assurance Component ID	Assurance Component Name
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing
AVA_MSU.2	Validation of analysis
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Independent vulnerability analysis

Annex C: Security Functional Requirements Results

Table 4. TOE security functional requirements.

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
Class FDP: User Data Protection	
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ETC.2	Export of user data with security attributes
FDP_IFC.2	Complete information flow control
FDP_IFF.2	Hierarchical security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_ITC.2	Import of user data with security attributes
FDP_RIP_DB.2	TOE full residual information protection
FDP_ROL.2	Advanced rollback
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_USB.1	User-subject binding
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of the TSF data
FMT_REV.1	Revocation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Class FPT: Protection of the TSF	
FPT_RCV.4	Function recovery
FPT_RVM_DB.1	TOE non-bypassability of the TSP
FPT_SEP_DB.1	Partial TSF domain separation

Annex D: Security Policy Details

- The TOE provides Discretionary Access Control (DAC), which restricts access to the objects based on the identity of the subjects and/or groups to which they belong.
- The TOE offers Mandatory Access Control (MAC), which restricts access to data objects based on the sensitivity of the information contained in the objects and the "clearance" of users to access such information.
- The TOE supports a security audit (Audit) function that recognizes and records security relevant activities.
- Identification and Subject Binding: Trusted RUBIX 5.0 identifies authorized users of a particular Trusted RUBIX 5.0 database by relying on Identification and Authentication (I&A) procedures of the underlying trusted operating system
- The TOE supports object reuse and ensures there is no deleted information that is accessible to a database user.
- The TOE supports secured import and export operations enabling the user to load data into the database, and extract data from the database into a text file.
- The TOE provides trusted recovery to a consistent and secure state from transaction failure and/or system failure.
- Security Management— The TOE supports five roles:
  - DBMS Audit Administrator: This role is responsible for administering the Trusted RUBIX audit subsystem and ensuring that all Trusted RUBIX users are accountable for their actions
  - Database Administrator: This role performs all operations that maintain the consistency and integrity of the stored data.
  - Database Operator: This role is responsible for performing database backups
  - Security Administrator (SA): This role is responsible for all operations, which may arbitrarily determine the label of a DBMS object.
  - Non-administrative DBMS User: This role has the Discretionary Access Control (DAC) permissions to use the Database.
- Protection of security functions
  - The reference monitor security function ensures that the TSF is always invoked before any functions are allowed to proceed
  - Domain Separation

Additional detail about the TOE security policy is contained in Annex D and within the [ST].

Annex E: Assumptions and Clarification of Scope

E.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL4 assurance requirements:

ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

E.2 Environmental Assumptions

The environmental assumptions listed in Table 5 are required to ensure the security of the TOE.

Table 5. Environmental assumptions.

Assumption	Description
A.ADMIN	It is assumed that database administrators, database operators, DBMS security administrators, and DBMS audit administrators are competent, and merit trust place in them.
A.USERS	It is assumed that authorized DBMS users are familiar with applicable DBMS security policies and procedures, and merit the trust placed in them.
A.DISASTER	It is assumed that the DBMS is protected against disasters such as loss of power, fire, flood, and destruction of facilities.
A.PHYSICAL	It is assumed that the DBMS, host OS, and IT environment are protected from physical attack.
A.SECURE_COMMS	It is assumed that the environment protects information while it is in transit between the DBMS and components of the IT environment.

E.3 Clarification of Scope

Table 6. Threats to the TOE.

Assumption	Description
T.ABUSE	An authorized DBMS user performs authorized actions that compromise (intentionally or otherwise) DBMS assets.
T.ADMIN_ERROR	An attacker may exploit vulnerabilities in the DBMS caused by improper administration of the DBMS in order to compromise DBMS assets.
T.ADMIN_ROGUE	A database administrator, DBMS security administrator, or DBMS audit administrator performs actions that intentionally compromise DBMS assets.
T.AUDIT_CORRUPT	An attacker may cause audit records to be lost or modified, or may prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.DOS	An attacker may exhaustively consume IT environment resources in order to deny DBMS assets to authorized DBMS users.
T.EAVESDROP	An attacker may gain unauthorized access to DBMS assets (e.g. authentication information or DBMS objects) when the data is transmitted to or from the DBMS.
T.EXPORT	An authorized DBMS user may send information (in soft or hard copy form) from DBMS objects to a recipient who is not authorized to see the information or who subsequently handles the information in a manner that is inconsistent with its sensitivity designation.
T.IMPROPER_INSTALLATION	An attacker may exploit vulnerabilities in the DBMS caused by improper delivery, installation, or configuration of the DBMS in order to compromise DBMS assets.
T.INSECURE_START	An attacker may exploit vulnerabilities in the DBMS created during start up or restart of the DBMS or host OS in order to compromise DBMS assets.
T.MASQUERADE	An attacker or external IT entity may masquerade as an authorized DBMS user or a external IT entity in order to gain unauthorized access to

Assumption	Description
	DBMS objects or DBMS resources.
T.POOR_DESIGN	An attacker may exploit vulnerabilities in the DBMS caused by unintentional or intentional errors in requirements specification, design or development in order to compromise DBMS assets.
T.POOR_IMPLEMENTATION	An attacker may exploit vulnerabilities in the DBMS caused by unintentional or intentional errors in implementing the design of the DBMS in order to compromise DBMS assets.
T.REPLAY	An attacker may gain unauthorized access to DBMS assets by replaying authentication information corresponding to an authorized DBMS user.
T.SPOOFING	An attacker may masquerade as the DBMS or an external IT entity in the IT environment and communicate with authorized DBMS users who incorrectly believe they are communicating with the DBMS or external IT entity.
T.SYSACC	An attacker may gain unauthorized access to the account of a database administrator, a database operator, a DBMS security administrator, a DBMS audit administrator, or other trusted personnel including IT environment administrators.
T.UNATTENDED_SESSION	An attacker may gain unauthorized access to DBMS assets using an unattended session of an authorized DBMS user.
T.UNAUTH_ACCESS	An attacker may gain unauthorized access to DBMS assets either via the DBMS itself or via the IT environment.
T.UNAUTH_MODIFICATION	An attacker may make unauthorized modifications to the DBMS security policy data or unauthorized use of security functions.
T.UNDETECTED_ACTIONS	In order to compromise DBMS assets, an attacker may successfully introduce vulnerabilities into the DBMS, or repeatedly exploit vulnerabilities in the DBMS, without being detected by the DBMS.
T.UNIDENTIFIED_ACTIONS	In order to compromise DBMS assets, an attacker may successfully introduce vulnerabilities into the DBMS, or repeatedly exploit vulnerabilities in the DBMS, without being identified by the DBMS audit administrator.
T.UNKNOWN_STATE	An attacker may exploit vulnerabilities in the DBMS created by a failure of the DBMS or host

Assumption	Description
	OS in order to compromise DBMS assets.
T.USER_CORRUPT	An attacker may make unauthorized deletions or modifications to DBMS data. Application note: In general, user authorizations are limited to specific DBMS objects (e.g., tables) and operations (e.g., read). Hence, the attackers in this threat may include authorized

Annex F: IT Product Testing

The COACT CCTL reviewed tests and test results applicable to the Trusted RUBIX 5.0 MLS RDBMS.

The Evaluation Team tested all TOE security functions and the majority of associated security functional requirements. The Evaluation Team used information provided in the developmental evidence to determine which interfaces to stimulate to produce the desired effects.

Software Test Environment:
The testing of Trusted RUBIX 5.0 is performed on an Intel platform.
Trusted RUBIX 5.0 relies on Trusted Solaris 8 to:

- Create and maintain users and groups.
- Create and maintain authorizations used for Role Based Access Control.
- Perform user-identification and authentication.
- Perform mandatory access control and discretionary access control between subjects and objects of the operating system. This includes protecting the Trusted RUBIX 5.0 database and audit log files at system high (Trusted RUBIX 5.0 explicitly sets them to system high at creation time).
- Provide reliable time stamps for audit event occurrence.
- Establish and manage the security lattice.

The Software Test Environment is designed for a high degree of automation and a minimum of operator interaction. The Trusted RUBIX 5.0 security tests are categorized (from largest to smallest) by test category, test suite, test group, test, and test step. The test category, test suite, and test group define the directory structure. The test and test step define the file structure. ITI has developed a set of testing tools to help execute automated and non-automated testing of the Trusted RUBIX 5.0 product. The runtest tool is used to execute the tests, other tools are used to generate, display, and archive the tests.

The *runtest* tool is used to execute the tests and produce basic results. It is executed upon a number of test directories (e.g., mac.d) and will execute all tests contained within. Prior to executing the contents of the test directories it will create a new database (*rgTest*) and execute an initialization SQL script (*DATA.sql*) upon the database. Prior to executing one test step (i.*, sh.*, c.* file) the *runtest* tool will set the user ID, group ID, clearance label, and session label of the process (using the u.* and l.* files). The test step is executed and the output from the execution is collected into an outcome file (o.*). The contents of the outcome file is compared, byte for byte, with a reference file (r.*) that was previously determined to be correct. If there are no differences between the two files the test is counted as succeeding and the output file is moved to a success file (s.*). If there is a difference between the two files the test is counted as failing and the output file is left unchanged. Therefore, if the test succeeds the success file (s.*) represents the actual results. If the test fails the outcome file (o.*) represents the actual results. The reference file (r.*) represents the expected results. Upon completion the *runtest* tools displays the

number of test steps that succeed and fail, along with their file names. It also gives cumulative results by test group directory.

Annex G: Security Target

The Security Target (ST) for Infosystems Trusted RUBIX Version 5.0 Multilevel Security Relational Database Management System is contained within the document Trusted RUBIX Version 5.0 Multilevel Security Relational Database Management System *Security Target,* Version 1.4.8, dated September 30, 2004, authored by Mitretek Systems, Inc. The ST is compliant with the *Specification of Security Targets* requirements found within Annex C of Part 1 of the CC [CCV2.1].

Annex H: Documentation

Table 7. Selected documentation.

Installation and Generation
Trusted RUBIX 5.0 Delivery and Operation, Version 1.4, September 26, 2004
Trusted RUBIX 5.0 Trusted Facility Manual, Version 1.5.1, January 15, 2004
Administrator and User Guidance
Administrator Guidance for Trusted RUBIX 5.0 Trusted Facility Manual, Version 1.5.1, January 14, 2004;
User guidance for Trusted RUBIX 5.0 Security Features User's Guide, Version1.4, January 29, 2004
SQL Reference Guide for Trusted RUBIX 5.0 Version 1.2, February 25, 2003

Additional documentation, most of which is proprietary, was available to the Evaluation Team during the evaluation of Trusted RUBIX V 5.0 MLS Relational Database Management System.

Annex I: Glossary

Table 8 is a glossary of terms used within this VR.

Table 8. Glossary.

Acronym	Expansion
CC	*Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.1, dated August 1999.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CCIMB	Common Criteria Interpretations Management Board
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I&A	Identification and Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

Annex J: Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap.nist.gov/cc-scheme).
- COACT CAFÉ Lab (http://www.coact.com)
- Infosystems Technology, Inc. (http://www.rubix.com)

CCEVS Documents

[CCV2.1] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999.

[CEMV1.0P2] *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Part 2: Evaluation Methodology, August 1999.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February 2000.

[CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0, March 2000.

[LSPP] Labeled Security Protection Profile, version 1.b, dated October 8, 1999

[MOSMPP] Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness, version 1.22, May 23, 2001

Other Documents

[ST] Trusted RUBIX Version 5.0 Multilevel Security Relational Database Management System Security Target, Version 1.4.8, dated September 30, 2004