National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Sybase Adaptive Server Enterprise, Version 12.5.2

Report Number: CCEVS-VR-05-0091
Dated: January 20, 2005
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

Introduction

This Validation Report is the source of detailed security information about the Sybase Adaptive Server Enterprise, Version 12.5.2, for any interested parties. Its objective is to provide practical information about the product or protection profile to consumers. The information in this Validation Report is obtained from the Evaluation Technical Report produced by SAIC evaluation team for Sybase Adaptive Server Enterprise, Version 12.5.2, and from the Security Target and Validated Product's List entry for this TOE.

Executive Summary

This report summarizes the validation of the evaluation of Sybase Adaptive Server Enterprise, Version 12.5.2. This Target of Evaluation (TOE) was evaluated against the security claims in its associated Security Target and found to be compliant with those claims. The particulars of this evaluation are as follows:

Evaluated Product: Sybase Adaptive Server Enterprise, Version 12.5.2

Evaluated by: SAIC

Completion Date: 20 January 2005

Common Criteria Version: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408

Interpretations applied as of: 5 May 2004

Evaluation Methodology: Common Methodology for Information Technology Security Evaluation, Version 1.0

Assurance Level: EAL 4 augmented with ALC_FLR.2

TOE Identification

The Target of Evaluation (TOE) is Sybase Adaptive Server Enterprise, Version 12.5.2, configured and operated according to the guidance documents identified in the Security Target. Adaptive Server Enterprise (ASE) is a Database Management System (DBMS) designed to execute as a set of applications in the context of commercially available operating systems, specifically Microsoft Windows 2000 (SP4), Microsoft Windows Server 2003, Sun Solaris version 8, (32- and 64-bit), IBM AIX 5L (32- and 64-bit), Hewlett-Packard HP-UX 11i (32- and 64-bit), Linux AS 2.1, and Silicon Graphics IRIX version 6.5.13 (32- and 64-bit). Adaptive Server Enterprise provides services to local and remote clients via the Tabular Data Stream (TDS) protocol.

ASE uses operating system services for process creation and manipulation; device and file processing; shared memory creation and manipulation; and security requests such as inter-process communication. The hardware upon which the operating system runs is completely transparent to ASE - ASE sees only the operating system's user interfaces.

The ASE Server is one or more operating system processes that service client requests. Multiple processes can be configured to enhance performance on multiprocessor systems. An ASE process has two distinct components, a DBMS component and a kernel component. The DBMS component manages the processing of SQL statements (data manipulation language - DML, data definition language - DDL, stored procedures and administrative commands), accesses data in a database, and manages different types of Server resources. The kernel component performs low-level functions for the DBMS component, such as task and engine management; network and disk I/O; and low-level memory management. Note that the TDS engine, that part of ASE that processes a TDS request, also uses the kernel component for low-level services. All of the ASE processes attach to one or more shared memory segments. The shared memory contains data structures that relate to task management and operating system services, caches of

database buffers, object descriptors, and other resources (e.g., other caches, queues, and stream I/O buffers) required to manage and process database commands.

Each client is associated with its own ASE task. In addition, there are several system tasks that perform specific services (e.g., tasks to write buffers to disk, tasks to write audit data to disk, and tasks to communicate with the network.).

Security Policy

ASE provides database management system (DBMS) services while it supports seven security functions upon objects in its scope of control:

Security audit: ASE has an audit mechanism that is invoked for access checks, authentication attempts, administrator functions, and at other times during its operation. When invoked, the date, time, responsible individual and other details describing the event are recorded to the audit trail.

The Audit log is stored as tables within ASE itself so that audit records can be protected from unauthorized access or modification. Furthermore, the SQL select command provided by ASE can be used by authorized administrators to effectively review the audit trail, including searching and sorting by user identities and other audit record attributes.

User data protection: ASE implements a Discretionary Access Control Policy over applicable database objects - databases, tables, views, and stored procedures. Note that there are other database objects that are either always private, always public, or are part of one of the afore-mentioned objects. In each case, the objects each have an owner which is initially the creator of the object.

Object owners have special permissions, while other users can subsequently be granted specific access permissions based on user identity, group memberships and active roles allowing applicable operations on objects. ASE also implements a Policy-based Access Control Policy over the content of database tables. This policy controls access based on Application Contexts of the current subject in conjunction with Access Rules associated with columns in database tables. This policy effectively allows access to be controlled on very specific and widely varying information about users.

Identification and authentication: ASE provides its own identification and authentication mechanism in addition to the underlying operating system. Users must provide a valid username and password before they can access any security-related functions. Once identified and authenticated, all subsequent actions are associated with that user and policy decisions are based on the users identity, group memberships and active roles.

Security management: ASE provides functions necessary to manage users and associated privileges, access permissions, and other security functions such as audit. The functions are restricted based on Discretionary Access Control Policy rules including role restrictions. While all of the administrative functions are available through and restricted at the TDS ASE Server interface, an application (isql) is provided to support ASE administrators. ASE defines a number of roles, but for the purpose of this evaluation every role that can manage the behavior of the applicable security functions is considered an authorized administrator (or trusted user) and all other users are simply referred to as users (or untrusted users).

Protection of the TSF: ASE protects itself from ASE subjects, from operating system subjects, and ensures that its policies are enforced in a number of ways. ASE depends on the underlying operating system to separate its processes from other operating system processes. ASE uses the discretionary access control mechanisms of the underlying operating system to protect TOE executables, TOE data, and TOE user data. ASE protects itself from ASE users and subjects by keeping its context separate from that of its users and also by makingeffective use of the operating system mechanisms to ensure that memory and files used by ASE have the appropriate access settings. Furthermore, ASE interacts with users through well-defined interfaces designed to ensure that the ASE security policies are always enforced. Operating system controls are part of the IT Environment and hence not evaluated as part of this evaluation.

Resource utilization: ASE provides resource limits to help authorized administrators prevent queries and transactions from monopolizing server resources. Specifically, authorized administrators can configure ASE to prevent queries and transactions that: exceed estimated or actual I/O costs, return too many rows, exceed the temporary database space allocated, and/or exceed a specified elapsed time.

TOE access: ASE allows authorized administrators to construct login triggers that can be used to restrict logins to a specific number of sessions as well as to restrict access based on time. ASE also allows authorized administrators to restrict access based on user identities.

Assumptions and Clarification of Scope

The Sybase Adaptive Server Enterprise runs as an application on a general purpose operating system, as described above. Users and buyers of the Sybase ASE should be prepared to operate a general purpose computing environment in a secure fashion, in order to provide protection for data and resources in ways the TOE cannot control.

Specifically, those responsible for the TOE should ensure that the following is true:

- Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.
- Appropriate physical security is provided within the domain for the value of the IT assets
- protected by the TOE and the value of the stored, processed, and transmitted information.
- The IT environment provides support commensurate with the expectations of the TOE.
- The environment protects network communication media appropriately
- The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation and applicable security policies and procedures by appropriately trained and trusted administrator personnel.

Evaluation Process and Conclusions

The evaluation team applied analysis of vendor-supplied evidence using SAIC-proprietary procedures, based upon work units described in the Common Evaluation Methodology. The vendor submitted evidence starting with the ST. The evaluation team documented their analysis and findings in an Evaluation Technical Report. As each section was finished, it was submitted to the NIAP Validator for review; if any deficiencies were found, they were noted and returned to the vendor for correction.

The evaluation team also performed four days of functional and vulnerability testing on the product in its installed configuration. All tests were documented for reproducibility, and results and deficiencies were noted. After a brief cycle, all deficiencies were rectified.

The conclusions of the evaluation team were a PASS for all the work units required for EAL 4 augmented with ALC_FLR.2 (flaw remediation).

Validation Process and Conclusions

The Validation of the Sybase ASE evaluation was performed by a Validator and a Technical Oversight Panel, comprising four additional validators. The Validator performed the routine analysis of the team's efforts via records review, ETR review, etc. The Validator attended the functional and vulnerability testing at the vendor site and observed the evaluation team's activities at first hand. The Validator also coordinated with the evaluation team and the

Technical Oversight Panel. The Validator conferred with the evaluation team by meeting, teleconference, and via encrypted e-mail when exchanging proprietary data.

Although several technical issues arose during the evaluation, there were no Observation Reports generated. The technical issues were all resolved by interaction between the Validator, Panel, and evaluation team.

The Technical Oversight Panel was convened twice; once to perform an in-depth analysis of the Security Target, and again to review the Development and Testing evidence as the evaluation team prepared to test the Sybase ASE. In both cases, the TOP produced a document of required and recommended changes to the Security Target and the testing plans. After the evaluation team performed testing, the Panel identified some areas for additional testing on the basis of known vulnerabilities and other areas.

Validator Comments/Recommendations

The Validator wishes to emphasize that, because the TOE is a software-only entity, customers and users of the TOE must exercise great care in protecting the TOE in its environment. The TOE can enforce protection only on the objects it directly controls, and can only protect itself from users and programs operating its own interface. It depends entirely on the base operating system in the proper configuration for protection of the TOE as a whole.

Annex A: Architectural Description of the TOE

Adaptive Server consists of two distinct modules:

- TDS Engine - The part of the Server which interprets and processes TDS requests, and formats responses according to the TDS protocol.
- T-SQL Engine - The part of the Server which performs the functions of a Database Management System, accepting and processing T-SQL commands and generating result sets.

The kernel provides services to the TDS Engine and the T-SQL Engine and is logically a part of both modules.

TDS Engine

The TDS Engine accepts as its only input messages formatted to the specification of the TDS protocol. TDS is used for transfer of requests and responses between clients and the Server. The TDS Engine receives the TDS request from the client in packets. It unbundles the request, and decides how the request should be resolved, based on its type. For each request the TDS Engine bundles the response in a packet and dispatches it to the requesting client.

T-SQL Engine

When a user connects to ASE, the T-SQL Engine activates any login trigger associated with the user after the TDS Engine has successfully processed the login record. After a user has logged in to the Server, the T-SQL Engine processes T-SQL commands that it receives from the TDS Engine, including:

- queries and DML commands (select, update, insert and delete)
- schema commands (create table, database, and others)
- stored procedure execution, including system stored procedures
- cursor commands
- set statements
- branching statements (if, while)
- transaction control statements

The T-SQL Engine generates result sets, individual return values and status as a result of executing T-SQL statements. It returns the results to the TDS Engine for formatting a response to the client's request according to the TDS protocol.

The T-SQL language restricts users from gaining access to data that has not been directly made available by the T-SQL Engine. For example, T-SQL has no equivalent to C-language pointers which give users access to all addressable memory. The T-SQL Engine limits a session's access to data based on its access control policies.

The Kernel

The kernel service abstracts the operating-system specific services for a consistent view regardless of the underlying operating system. The T-SQL Engine and the TDS Engine use kernel services in the following areas:

- Engine Management
- Task Management
- Memory Management
- Network I/O
- Disk I/O
- Initialization, Startup and Shutdown

Annex B: Assurance Requirements Results

This section documents the assurance requirements that the IT product satisfies. A detailed description of these requirements, as well as the details of how the product meets each of them can be found in the Security Target. This section highlights all the augmentations to the EAL.

ACM: Configuration management

- ACM_AUT.1: Partial CM automation
- ACM_CAP.4: Generation support and acceptance procedures
- ACM_SCP.2: Problem tracking CM coverage ADO: Delivery and operation

ADO: Delivery and Operation

- ADO_DEL.2: Detection of modification
- ADO_IGS.1: Installation, generation, and start-up procedures

ADV: Development

- 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: Guidance documents

- AGD_ADM.1: Administrator guidance
- AGD_USR.1: User guidance

ALC: Life cycle support

- ALC_DVS.1: Identification of security measures
- ALC_FLR.2: Flaw reporting procedures (augmentation)
- ALC_LCD.1: Developer defined life-cycle model
- ALC_TAT.1: Well-defined development tools

ATE: Tests

- ATE_COV.2: Analysis of coverage
- ATE_DPT.1: Testing: high-level design
- ATE_FUN.1: Functional testing
- ATE_IND.2: Independent testing - sample

AVA: Vulnerability assessment

- 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

This section documents the SFRs that the TOE satisfies and highlights extended functional requirements. A detailed description of these requirements, as well as the details of how the product meets each of them can be found in the ST.

Several requirements are repeated and marked with a suffix “a”, “b”, etc. These are iterations, requirements repeated with the text altered

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.3: Action in case of possible audit data loss

FDP: User data protection

- FDP_ACC.1a: Subset access control
- FDP_ACC.1b: Subset access control
- FDP_ACF.1a: Security attribute based access control
- FDP_ACF.1b: Security attribute based access control
- FDP_RIP.2a: Full residual information protection

FIA: Identification and authentication

- FIA_AFL.1: Authentication failure handling
- FIA_ATD.1: User attribute definition
- FIA_SOS.1: Verification of secrets
- FIA_UAU.2: User authentication before any action
- FIA_UAU.7: Protected authentication feedback
- FIA_UID.2: User identification before any action
- FIA_USB.1: User-subject binding

FMT: Security management

- FMT_MOF.1: Management of security functions behaviour
- FMT_MSA.1: Management of security attributes
- FMT_MSA.2: Secure security attributes
- FMT_MSA.3: Static attribute initialization

- FMT_MTD.1a: Management of TSF data
- FMT_MTD.1b: Management of TSF data
- FMT_MTD.1c: Management of TSF data
- FMT_REV.1a: Revocation
- FMT_REV.1b: Revocation
- FMT_SMF.1: Specification of Management Functions (per
- International Interpretation #65)
- FMT_SMR.1: Security roles

FPT: Protection of the TSF

- FPT_RVM.1a: Non-bypassability of the TSP
- FPT_SEP.1a: TSF domain separation

FRU: Resource utilization

- FRU_RSA.1: Maximum quotas

FTA: TOE access

- FTA_MCS_EXP.1: Basic limitation on multiple concurrent sessions
- FTA_TSE.1: TOE session establishment

Annex F: IT Product Testing

The evaluation team executed the entire set of vendor test procedures per the evaluated configuration as described below. The evaluation team used two platforms to perform its testing – Windows 2000 and Sun Solaris. The evaluation team chose these two platforms to perform its testing because the source code is different between Windows and Unix machines, so Windows needed to be part of the evaluation team subset. The Solaris machine was selected since it is representative of the remaining Unix platforms. All of the security code on all of the Unix platforms is identical. The only source code differences among the Unix platforms are Kernel services (process handling, signal handling, network IO, disk IO, etc).

The following configurations were used to create the test environment:

- Test machine 1
    1. Solaris 2.8
    2. ASE version 12.5.2
    3. QuaSR driver and QuaSR agent
- Test Machine 2
    1. Windows 2000 SP4

2. ASE version 12.5.2
3. QuaSR agent

The vendor created a test suite for each of the following testing areas. The test documentation includes Sybase ASE Common Criteria Test Plan, a TSQL correspondence matrix that maps the TSQL commands to the test cases, and test suites for all the security function in the Security Target. The test suites included are:

- Identification and Authentication
- Row Level Access Control
- Auditing
- Discretionary Access Control (DAC)
- Resource Governor
- Dynamic Reconfiguration
- Groups and System Defined Roles
- User Defined Roles
- Configuration Interfaces
- isql (Interactive SQL parser)
- ASE Self Protection
- Security Management Functions
- Object Reuse Prevention
- Tabular Data Stream (TDS).

Vendor also performed tests on the raw Protocol Data Unit (PDU) Interface and Tabular Data Stream (TDS) Interface for security and robustness by using a rogue client that posted malformed queries to the ASE Server. In all cases, the behaviour of ASE was found to be secure and accurate.

Each specific test suite includes a description of the intent of the test suite and the testing approach. The specific test suites also include the test case description, the test procedures, and the expected results. During its initial review, the evaluation team found the test coverage to be almost complete. Additional information was required for a few test cases and more information was required about running the test suites.

Actual results were provided for all platforms claimed in the security target. The evaluation team sampled these results and ensured that the tests were producing the documented results. The evaluation team ran the vendor-supplied manual procedures for the Self Protection tests on the Solaris and Windows machines.

Evaluation Team Testing

The evaluation team generated its own tests for additional functional testing and for vulnerability testing. The team created 11 additional functional tests to supplement the vendor test suite.

The vulnerability test cases were derived using two methods. The first method extends the developers vulnerability analysis. The other tests were developed by the evaluation team using a flaw hypothesis method. Evaluation team members devised tests based upon examination of the evaluation evidence.

Vulnerability Testing generated 11 test cases that passed in that the Sybase Adaptive Server Enterprise resisted the attack or prompted a minor fix.

Annex G: Security Target

Sybase Adaptive Server Enterprise Security Target, Version1.0, dated 11/8/2004

Annex H: Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation

Object Reuse Design Specification	4/30/2004
Object Reuse Prevention Functional Specification	10/27/2004
Discretionary Access Control Functional Specification	11/09/2004
Access Control List Management Design Specification	11/05/2004
Policy Based / Row Level Access Control Functional Specification	11/02/2004
Policy Based / Row Level Access Control Design Specification	10/08/2004
Groups and System Defined Roles Functional Specification	09/20/2004
Groups and System Defined Roles Design Specification	04/05/2004
User Defined Roles Functional Specification	09/20/2004
User Defined Roles Design Specification	04/20/2004
Resource Governor Functional Specification	10/12/2004
Resource Governor Design Specification	10/12/2004
ASE Self Protection Functional Specification	11/24/2004
ASE Self Protection Design Specification	11/12/2004
Adaptive Server Enterprise Architecture Summary	09/20/2004
Adaptive Server Enterprise Auditing Functional Specification	10/27/2004
Adaptive Server Enterprise Auditing Design Specification	10/27/2004
Identification and Authentication Design Specification	10/08/2004
Identification and Authentication Functional Specification	09/20/2004
Security Management Functions Functional Specification	03/30/2004
Configuration Interface Functional Specification	04/01/2004
Configuration Interface Design Specification	04/01/2004
Reference Validation Mechanism Design Specification	11/5/2004
Dynamic Reconfiguration Design Specification	03/19/2004
Dynamic Reconfiguration Functional Specification	03/19/2004
TDS 5.0 Functional Specification, Version 3.6	06/2002
ISQL Functional Specification	03/19/2004
T-SQL Correspondence	10/29/2004
Adaptive Server Enterprise Security Policy Model	11/02/2004
Implementation Subset Representation	

Guidance documentation

Common Criteria Evaluation Road Map	Release bulletin for 12.5.2
Configuration Guide Adaptive Server Enterprise for UNIX	November 2004
Configuration Guide Adaptive Server Enterprise for Windows NT	November 2004
Sybase ASE 12.5.1 System Administration Guide	November 2004
Sybase ASE 12.5.1 Reference Manual: Commands	November 2004
Sybase ASE 12.5.1 Reference Manual: Procedures	November 2004

Configuration Management and Lifecycle documentation

Sybase Adaptive Server Enterprise Configuration Management Plan	v 0.3	11/24/2004

Delivery and Operation documentation

Supplement for Installing Adaptive Server for Common Criteria Configuration, Document ID: DC00080-01-1252-01, Last revised: November 2004
Sybase Adaptive Server Enterprise Delivery and Operation Procedures v 0.1 04/30/2004
Installation Guide Adaptive Server Enterprise for Digital UNIX
Installation Guide Adaptive Server Enterprise for HP-UX
Installation Guide Adaptive Server Enterprise for IBM RISC System/6000 AIX
Installation Guide Adaptive Server Enterprise for Linux/Intel
Installation Guide Adaptive Server Enterprise for Silicon Graphics IRIX
Installation Guide Adaptive Server Enterprise for Sun Solaris
Installation Guide Adaptive Server Enterprise for Windows NT
Supplement for Installing Adaptive Server for Common Criteria Configuration

Test documentation

Sybase ASE Common Criteria Test Plan v4.0	11/17/2004
Test Suite Documents and associated tests	
Identification and Authentication	04/27/2004
Row Level Access Control	11/11/2004
Auditing	11/10/2004
Discretionary Access Control (DAC)	11/10/2004
Resource Governor	11/10/2004
Dynamic Reconfiguration:	11/11/2004
Groups and System Defined Roles	07/12/2004
User Defined Roles	07/12/2004
Configuration Interfaces	07/12/2004
isql (Interactive SQL parser)	07/12/2004
ASE Self Protection	11/09/2004
Security Management Functions	07/06/2004
Object Reuse Prevention	07/10/2004
Tabular Data Stream (TDS)	11/04/2004
Test Mapping to Design Specifications	11/08/2004
T-SQL Correspondence	11/01/2004
Actual Test Results for all OS platforms	11/04/2004

Vulnerability Assessment documentation

Sybase ASE Vulnerability Analysis v 1.1 11/05/2004