Trust Technology Assessment Program

Validation Report

SuperNet 2000 EAL4/r1

TTAP Report Number: TTAP-VR-0016

Edition 1

October 2000

Prepared By:
Trust Technology Assessment Program (TTAP)
National Security Agency (V13)
9800 Savage Road, Suite 6740
Ft. George G. Meade, MD 20755-6740

Arrangement
on the
Recognition of Common Criteria Certificates
in the field of
Information Technology Security

The Trust Technology Assessment Program (TTAP) Oversight Board is a member of the above Arrangement. As such, it confirms that a Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and that the certificate has been issued in accordance with the terms of this Arrangement. The judgements contained in the evaluation and this Validation Report are those of the Oversight Board which issues it and of the evaluation facility which carried out the evaluation. There is no implication of acceptance by Members of the Arrangement of liability with respect to judgements or losses sustained as a result of reliance placed upon information contained herein.

Executive Summary

Production and evaluation of the SuperNet 2000 EAL4/r1, was sponsored by Electronic Engineering Systems, Inc., 1200 North Battlefield Boulevard, Suite 120, Chesapeake, VA 23320.

This TOE meets the Common Criteria Scheme Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (ARCC). The TOE evaluation was completed in October 2000 by the SAIC Common Criteria Testing Laboratory (CCTL) (an accredited Trust Technology Assessment Program (TTAP) evaluation facility in the United States) and has been shown to be conformant with Part 2 and Part 3 of the Common Criteria for Information Technology security Evaluation, version 2.1 (CCv2.1) requirements for TOEs. The Common Evaluation Methodology version 1.0 was used to conduct the TOE evaluation to show conformance to CCv2.1 Part 3 Evaluation Assurance Level (EAL) 4.

1.0 Identification

Section 2.1 of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) contains the identification information.

2.0 Security Policy

Sections 2.1 (ST and TOE Identification), 2.4 (Target of Evaluation Overview), 3.1 (Physical TOE Description), 3.2 (TOE Architecture Model) and 6.1 (TOE Security Functional Requirements) of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) contains the descriptions of the SuperNet 2000 EAL4/r1 security policy.

3.0 Assumptions and Clarification of Scope

3.1 Usage & Environmental assumptions

Section 4.1 (Secure Usage Assumptions) of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) documents the usage assumptions made about the SuperNet 2000 EAL4/r1 during the evaluation.

3.2 Clarification of scope

Section 3.1 (Physical TOE Description) specifies the threats that the SuperNet 2000 EAL4/r1 does not counter. The SuperNet 2000 EAL4/r1 is not expected to:

- Provide complete information flow protection from one operating domain to another, since certain devices are active when either UDD[1] is active.
- Provide security features and controls (e.g., operating system, file access controls) necessary for a user to interact with a specific operating environment.

4.0 Architectural Information

Sections 2.1 (ST and TOE Identification), 2.2.1.2 (Terminology specific to the TOE), 2.4 (Target of Evaluation Overview), 3.1 (Physical TOE Description), 3.2 (TOE Architecture Model), and 3.3 (Logical Scope and Boundary) of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) provides the architectural information for the SuperNet 2000 EAL4/r1.

1. See section 2.2.1.2 on page 5 of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) for a definition of the term User Data Domain (UDD).

5.0 Documentation

The documentation provided with the SuperNet 2000 EAL4/r1 is:

- SuperNet 2000 EAL4/r1 Administrator Guide.
- SuperNet 2000 EAL4/r1 Quick Reference Guide.
- SuperNet 2000 EAL4/r1 User Reference Guide.

6.0 IT Product Testing

The SuperNet 2000 EAL4/r1 was tested to the configuration that is specified in the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4), SuperNet 2000 EAL4/r1 Administrator Guide, and SuperNet 2000 EAL4/r1 Delivery and Operation.

The TSF of the SuperNet 2000 EAL4/r1 is a hardware security enforcing mechanism. The testing conducted focused on physically testing the connections, the cabinets, and the locks.

6.1 Developer testing

The developers testing ensured that all the security requirements as defined in the ST are tested. The developer:

- Identified all of the Security Functional Requirements (SFRs) satisfied by the TOE that are identified in the ST,
- Identified all of the TOE Security Functions (TSF) identified in the ST,
- Mapped all SFRs to the TSF to demonstrate that if all TSF are tested, all SFRs will be tested,
- Identified the security relevant external interface that test the security relevant features of each TSF,
- Identified the properties of each external interface identified above that need to be tested to ensure that all security relevant properties of each identified interface are tested.

The test plan included sections that address both breadth and depth of coverage for testing.

Electrical connection testing occurs at the DSS[1] and at the electrical interface for devices that are specific to one UDD (i.e., floppy drive, nic cards, and hard drives). When testing the DSS, DSS test positions are identified in tests as Public (P), Interim (I), and Restricted (R). Voltages are tested at each device when the UDD Position P, I and R are each selected.

1. See section 2.2.1.2 on page 4 of SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) for a definition of the term Domain Selection Switch (DSS).

Once the DSS electrical positions are tested, electrical connectivity at each device is also tested. The test plan includes a table showing the DSS pin connections to specific devices attached to a specific UDD. For each device, voltage is checked at the appropriate DSS pin and at the electrical input for the device. Sufficient voltage is expected when the DSS is selected at the position for which that device is dedicated to. Insufficient voltage is expected otherwise.

Test cases are provided to ensure that the TOE cabinet case cannot be removed without unlocking the TOE cabinet lock.

Section 7.4.1.6 (Testing) of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) specify more information on testing of the SuperNet 2000 EAL4/r1.

The results of the developer testing showed that the SuperNet 2000 EAL4/r1 is capable of enforcing the security functionality specified in the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4).

6.2 Evaluator testing

.The evaluator testing entailed re-running the developers testing and conducting their own developed tests. The evaluation team devised a set of tests based on a review of the evaluation evidence focusing on the high-level design, low-level design, test documentation, user guidance, and administrator guidance.

The test were structured to determine if the UDD selection only can be accomplished through the DSS, that only one UDD selection requires a physical key authentication device to be inserted into the DSS, that the DSS connections to hardware devices within the workstation cannot be modified, since they are protected by a specially constructed, locked cabinet, and to attempt to gain access to the TSF through non-TSF TOE external interfaces.

The results of the evaluator testing showed that the SuperNet 2000 EAL4/r1 is capable of enforcing the security functionality specified in the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4).

7.0 Evaluated Configuration

The SuperNet 2000 EAL4/r1 is delivered in the evaluated configuration. Two domains are in the evaluated configuration an “Unsecure” and a “Secure” domain.

The “Unsecure” domain which is the default domain for the SuperNet 20000 EAL4/r1 may be accessed by anyone that has physical access to the SuperNet 2000 EAL4/r1. No key and switching is necessary to access this domain. The “Unsecure” domain in the evaluated configuration is represented by a green light emitting diode (LED).

The “Secure” domain is the controlled access domain for the SuperNet 20000 EAL4/r1. A user must possess a key to switch to the “Secure” domain. the “Secure” domain in the evaluated configuration is represented by a red light emitting diode (LED).

The SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4), the administrator, and user guide should be consulted for more information on the evaluated configuration.

8.0 Results of the Evaluation

The SuperNet 2000 EAL4/r1 was evaluated to EAL4. Section 6.2 (Security Assurance Requirements), Table 8, of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) has a listing of the assurance components that have been satisfied.

Sections 6.2 (Security Assurance Requirements), AVA_SOF.1, and 7.4 (Assurance Measures) contains a detailed description of how the SuperNet 2000 EAL4/r1 meets each of the assurance requirements.

9.0 Comments and Recommendations

The SuperNet 2000 EAL4/r1 evaluation did not deal with the information flow aspects of a switch. The requirement set specified in the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) models an access control policy. The access being controlled is access to certain devices dependent on which domain a user is in. Since information flow requirements are not in the ST they were not evaluated during the evaluation. The SuperNet 2000 EAL4/r1 does not provide complete information flow protection from one operating domain to another so the potential exist that information could flow from one operating domain to another.

10.0 Security Target

The SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) is considered part of this document. It is considered a separate annex.

11.0 Glossary

Assurance - Grounds for confidence that an entity meets its security objectives.

Class - A grouping of families that share a common focus.

Component - The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Element - An indivisible security requirement.

Evaluation - Assessment of a PP, an ST or a TOE, against defined criteria.

Evaluation Assurance Level (EAL) - A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Package - A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Protection Profile (PP) - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Target of Evaluation (TOE) - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Section 2.2.1 (Terminology) of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) contains more definitions related to the TOE and the SuperNet 2000 EAL4/r1 evaluation.

12.0 Acronyms

- ARCC Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.
- CC Common Criteria version 2.1.
- CEM Common Evaluation Methodology version 0.6 for part 1 and 1.0 for part 2.
- PP Protection Profile.
- PSS Peripheral Sharing Switch for Human Interface Devices.
- TTAP Trust Technology Assessment Program.

13.0 Bibliography and References

- Common Criteria, version 2.1, Part 1, CCIMB-99-031.
- Common Criteria, version 2.1, Part 2, CCIMB-99-032.
- Common Criteria, version 2.1, Part 3, CCIMB-99-033.
- Common Evaluation Methodology, version 0.6, Part 1, CEM-97/017.
- Common Evaluation Methodology, version 1.0, Part 2, CEM-99/045.
- http://www.radium.ncsc.mil/tpep/
- http://niap.nist.gov/
- http://niap.nist.gov/cc-scheme/
- http://www.commoncriteria.org/

- Table 12 (EAL4 Assurance Evidence) of the SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4) has a listing of the developer provided evaluation evidence and documentation.