NISTIR 5810

The TMACH Experiment Phase I - Preliminary Developmental Evaluation

Ellen Colvin Flahavin

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

Sponsored by:

Advanced Research Projects Agency

NIST

NISTIR 5810

The TMACH Experiment Phase I - Preliminary Developmental Evaluation

Ellen Colvin Flahavin

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

Sponsored by:

Advanced Research Projects Agency

June 1996

U.S. DEPARTMENT OF COMMERCE
Michael Kantor, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arati Prabhakar, Director

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose of Report

This document describes the multi-national evaluation experiment of the Trusted Mach system. This report focuses on Phase I - The Developmental Evaluation Phase. The objective is to provide an historical journal discussing the experiment, and providing insight into what has been learned and accomplished thus far. Discussed are the objectives of the effort, the participants, how the evaluation has proceeded, and the benefits.

1.2 Purpose of the Experiment

In 1983, the U.S. Department of Defense published the Trusted Computer System Evaluation Criteria (TCSEC). Since that time, the National Computer Security Center has been performing trusted system evaluations within the United States. In 1990, the Commission of European Communities published a draft version of a European developed criteria, the Information Technology Security Evaluation Criteria (ITSEC), that generalized and modified the TCSEC. Evaluations against the ITSEC were to be performed by Commercial Licensed Evaluation Facilities (CLEFs) that were controlled by National Authorities. Considerable debate ensued on how the TCSEC and ITSEC compared but the debate remained at a philosophic level for want of hard evidence based upon comparative evaluation experience. Although claims were made that the criteria were compatible with one another, there appeared to be no real basis for discussing reciprocity of rating among the various countries. If an ITSEC-rated systems were to be proposed for use within NATO, the United States would have little understanding of the rating.

The Trusted Mach (TMach) system, targeted at a B3 TCSEC rating, was being developed under the U.S. Advanced Research Projects Agency (ARPA) funding at this time. Evaluation of the TMach system against both the ITSEC and TCSEC was suggested as a means for understanding how the criteria and their accompanying evaluation processes compared. Although the TMach evaluations would not definitively answer how the criteria compared at all levels, it would move the comparison into a concrete rather than philosophic discussion. By actually evaluating TMach against the criteria, the different requirements of each criterion and evaluation process would become visible.

It is in the interest of the U.S. Government to understand how these two criteria differ in practice and how evaluations done under each may be compared. Efforts to reconcile the differences have been undertaken based upon detailed knowledge and understanding gained thus far. North America and Europe have agreed to develop a Common Criteria for Information Technology Security Evaluation.

1.3 Project Authorization

In November 1990, James Burrows, then the Director of the Computer Systems Laboratory of the National Institute of Standards and Technology (NIST), met with European officials and Steve Walker of Trusted Information Systems to discuss initiating a preliminary developmental evaluation of TMach against the ITSEC. As a result of this meeting, NIST finalized an agreement with the ARPA to coordinate and oversee the TMach evaluation work to be done by Germany and the United Kingdom (UK).

Under the agreement, NIST received funds from ARPA for the evaluations and negotiated the contracts with appropriate organizations in those countries. NIST monitors the TMach evaluation contract performance for ARPA, and provides the contractual and management interface with the U.S. Government. NIST is responsible to ARPA as the U.S. Government agent for setting the evaluation tasks and coordinating the evaluation work.

1.4 Project Scope

On December 20, 1990, NIST published Commerce Business Daily (CBD) announcements notifying potential contractors of the solicitations for the TMach evaluation work. The intent of the contract work is to gain further understanding of the ITSEC and its evaluation process. The ITSEC evaluations of TMach began in September of 1991. These multiple evaluations have been undertaken with the objective of understanding the different criteria and evaluation processes by seeing how they relate to a single system.

TMach, which will provide users with both high level trust and a Unix interface, is under evaluation by three different nations against two separate criteria. In the U.S., TMach is being evaluated at the B3 level against the TCSEC, and concurrent evaluations of TMach at F-B3/E5 against the ITSEC.

1.5 References

BSI CERTIFICATION - Procedural Description- BSI 7125, April 1994.

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC), Department of Defense, DoD 5200.28-STD, December 1985.

INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA (ITSEC), Version 1.2, Commission of the European Communities, 28 June 1991.

INFORMATION TECHNOLOGY SECURITY EVALUATION MANUAL (ITSEM), Version 1.0, Commission of the European Communities, 10 September 1993.

MANUAL OF COMPUTER SECURITY EVALUATION, UKSP 05, Part III, Issue 1.0, UK IT Security Evaluation and Certification Scheme Certification Body, 1 June 1994.

TRUSTED MACH EVALUATION WORK PROGRAMME, S. H. Hill, J.C. Straw, 6 December 1991.

TRUSTED MACH SECURITY TARGET, Trusted Information Systems, Inc., 1992.

TRUSTED MACH SYSTEM ARCHITECTURE, Trusted Information Systems, Inc., September 23, 1991.

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME, UKSP 05, Part II, Standard Evaluation Work Programmes, Issue 1.0, UK IT Security Evaluation and Certification Scheme Certification Body, 14 December 1994.

2. OVERVIEW OF THE TMACH SYSTEM ARCHITECTURE

The Trusted Mach (TMach) system is a secure server-based operating system implemented as a message passing microkernel and a set of servers. The servers provided operating system functionality that is traditionally found in the operating system kernel. The TMach system is layered in accordance with generally accepted software engineering principles. These principles require that abstract layers depend upon primitive layers and that the primitive layers shall not depend upon the abstract layers. TMach is designed to support information systems security and control requirements. Each protection layer provides abstractions and services to the layers above. Communication between the protection layers is performed over well-defined interfaces. Each individual component defines a separate task. Layers of tasks are used in order to protect the trusted computing base (TCB). Dependencies between the components, whether microkernel modules or TCB tasks, is strictly downwards, with no component depending on a higher component for its functionality.

3. EVALUATION CRITERIA AND METHOD

3.1 ITSEC

In May 1990, four members of the European Community, specifically the governments of France, Germany, the Netherlands, and the United Kingdom, developed a harmonized computer security evaluation criteria referred to as the ITSEC. The purpose of producing an international harmonized criteria was to accomplish international mutual recognition of evaluation results.

3.2 Scheme

In Europe, evaluations under the ITSEC are performed by commercially licensed facilities. Such facilities are managed and staffed by commercial organizations (parent companies) which have been licensed under the nation's Scheme, and a condition of license is that the facility must also be accredited by the nation's accreditation body .

These facilities are subject to the rules of operation which forms part of the License Agreement. These rules govern:

a. Licensing and Re-licensing of facilities;

b. Security and Confidentiality;

c. Quality and Management;

d. Staff Qualifications and Training.

Licenses are granted to interested commercial companies which have been successfully assessed with regard to Quality, Management, Security and Technical Expertise.

3.3 ITSEM

The German/United Kingdom evaluation methodologies respectively were identified as approaches to the TMach evaluation. Early in 1992, a draft of the ITSEM was completed by the same EC Member Nations which prepared the ITSEC to establish a common evaluation process to be used with the ITSEC. The ITSEC forms a companion piece for the conduct of product evaluations. The ITSEM contains a sufficient amount of information on evaluation, methods and procedures to enable technical equivalence of evaluations performed in different environments to be demonstrated.

4. ROLES AND OBJECTIVES

4.1 Governments

ARPA - United States

ARPA's objective is to advance the technology of computer systems for the Department of Defense. The TMach Project began in the late-eighties with ARPA desiring a trusted operating system based upon the highly portable Mach microkernel. Through the ITSEC evaluation of the TMach system, ARPA will gain the knowledge to understand how ITSEC and TCSEC evaluations compare, information that may be essential to determine the acceptability of candidate NATO systems. The project provides insight to guide decisions for evaluation reciprocity. It will also result in a trusted operating system, TMach, that has been evaluated against both criteria and thus should be acceptable for both the United States and European markets. Also, the trust characteristics of TMach will fit into ARPA's evolutionary operating system goals.

This experiment is scheduled as a four year effort level before going to formal evaluation.

NIST - United States

NIST is responsible to ARPA as the U.S. Government agent for setting the evaluation tasks and coordinating the evaluation work. The benefits of this relationship include understanding of the practical differences between the ITSEC and the TCSEC, the opportunity to compare the evaluations done under each, the creation of worked examples to the ITSEC style of evaluations, and exploration of the practical aspects of reciprocity with the U.S. gaining an understanding of the European Process.

CESG/DTI - United Kingdom

CESG intends to continue a joint operation to certify the results of evaluations of systems and products to common technical standards, and to deal with other nations on the mutual recognition of such certificates.

BSI/GISA - Germany

The two major project objectives are performing a concurrent E5-evaluation and research on harmonization aspects. GISA has already gained experiences with ITSEC-evaluations, but because the TMach Project will be one of the first to reach an E5-level in a product evaluation, many questions will be answered concerning a common European interpretation of the criteria for concurrent evaluation.

4.2 Developer

TIS - United States

TIS built TMach on the Mach microkernel, which was developed by Carnegie Mellon University (CMU) and used by the Open Software Foundation (OSF) as their future standard. TIS built a proof of concept prototype, submitted it to the National Security Agency (NSA) for a B3 evaluation, and came up with the idea of having a joint evaluation to compare the ITSEC and TCSEC. Among TIS's expectations are to evaluate the TMach architecture and trust strategy, to evaluate the TMach development process and practices, and to understand the similarities and differences between the evaluation criteria and evaluation process.

4.3 Observers

NSA - United States

NSA agreed on the importance of achieving mutual recognition of different evaluation approaches and emphasized that no organization wants to initiate a dozen different reciprocity agreements. Concern was expressed regarding implications of government funded vs. commercially funded evaluations and the maintenance of certification quality.

OSF - United States

OSF is composed of several international member companies, all interested in U.S./EC evaluations of OSF offerings. OSF wants two questions answered. First, when developing very high security in an operating system, will the system meet adequate performance goals? Second, will adequate security meet market requirements?

SCSSI - France

SCSSI will become a certifying body in the near future. They believe the TMach project is an interesting one and are pleased to be invited to the meetings. Their national vendors have an interest, and support from SCSSI will continue in the form of attending these meetings.

CSSE - Canada

Canada's interest in TMach is in the harmonizing of criteria, and in the reciprocity issues.

4.4 Evaluators

IABG in Germany, Logica, and Secure Information Systems Limited in the UK are the facilities chosen to perform the evaluations.

5. DESCRIPTION OF EVALUATION

The current TMach evaluation is a concurrent evaluation, meaning that system development and evaluation are on-going at the same time. This form of evaluation was chosen since the criteria and evaluation processes were relatively unknown. With a concurrent evaluation there is an opportunity to make changes if issues exist.

A constraint on the evaluation is that not all of the deliverables necessary for an E5 evaluation are available. The evaluation is thus limited to those activities which may be performed using the available deliverables, both in terms of correctness and effectiveness. The main part of the evaluation is devoted to an examination of the Requirements, the Architecture and Detailed Design, and examination of Development of Procedures and Practices, as well as evaluators' assessment of the security target, the mathematical model, and the developer's effectiveness analysis.

An additional constraint on the evaluation is that an upper limit is placed on the total evaluation effort (as funded by the sponsor of the evaluation). This means that the assurance of correctness or effectiveness obtained from an examination of those deliverables that are available may not necessarily be sufficient for Level E5.

Since this is a concurrent evaluation, and the dates on which the various deliverables are available may be subject to change, it is anticipated that the Evaluation Work Program (EWP) may need to undergo a number of revisions to reflect any changes in the schedule.

6. RELEVANT EVALUATION DELIVERABLES

The Development Process
Requirements

- The security target for the Target of Evaluation (TOE)
- Definition of or reference to an underlying formally specified model of security
- Informal interpretation of the underlying model in terms of the security target

Architectural Design

- Semiformal description of the architecture of the TOE
- Semiformal description of the High Level Design and the Detailed Design

Implementation

- Test Documentation
- Library of test programs and tools used for testing the TOE
- Source code or hardware drawings for all security enforcing functions and security relevant components

The Development Environment

- Configuration list identifying the version of the TOE for evaluation
- Information on the configuration control system and its tools
- Audit information on modifications of all objects of the TOE subject to configuration control
- Information on the acceptance procedure
- Information on the integration procedure
- Information on the security of the development environment
- Description of all implementation languages and compilers used
- Source code of all runtime libraries used

Operation

- User documentation
- Administration documentation

Operational Environment

- Delivery and Configuration documentation
- Start-up and Operation Documentation

Effectiveness Criteria - Construction

- Suitability Analysis
- Binding Analysis
- Strength of Mechanisms Analysis
- List of known vulnerabilities in Construction

Effectiveness Criteria - Operation

- Ease of Use Analysis
- List of known vulnerabilities in Operational Use

7. ASSESSMENT OF APPROACH

The section defines the approach taken for this concurrent evaluation.

a) An Evaluation Work Program (EWP) was written to form the detailed plan for the full evaluation of TMach, containing detailed specifications of individual Work Packages, timescales, resources required, and any assumptions or constraints on the evaluation.

b) A Deliverables List accompanies the EWP and identifies all deliverable required for the evaluation (given a target evaluation level of E5), providing a mapping of the available deliverables on to the ITSEC E5 requirements.

c) Evaluation Technical Reports contain the report of the assessment of the security target, the security policy model, implementation, development environment, operation and effectiveness for TMach against the ITSEC E5 and F-B3 requirements.

8. WORK PERFORMED AND RESULTS OBTAINED

The evaluators have carried out an evaluation of the various aspects of the TMach development process, as follows:

a) A complete evaluation of the TMach security target has been performed. This has confirmed that the ITSEC E5 requirements can be satisfied, subject to the clearance of a small number of minor errors. The security target's claimed compliance with ITSEC F-B3 has been confirmed.

b) The TMach security policy model has been evaluated against ITSEC E5, identifying some minor problems.

c) The evaluators have assessed the TMach architectural design against ITSEC E5. This has identified further requirements for evidence in terms of the use of semiformal notations and of traceability of SEFs at this level.

d) High Level Design documents have been reviewed for the majority of the trusted servers. A sample of the low level design documentation has also been evaluated, together with an assessment of TIS's approach to traceability of SEFs at this level. The evaluation has highlighted areas where more evidence may be needed at this level, in order to satisfy ITSEC E5.

e) A sample of the source code has been examined, indicating that there should be no major problems in terms of satisfying the E5 requirements in this area. TIS's proposed approach to testing, and provision of test evidence, has been assessed and discussed. An agreed interpretation of the ITSEC and ITSEM requirements has been reached.

f) The TMach development environment has been subjected to a preliminary assessment against ITSEC E5, providing feedback on the likelihood of the ITSEC E5 requirements being satisfied. The assessment has identified areas where further evidence and assessment will be required.

The evaluation results have provided a basis for detailed discussions of the ITSEC E5 requirements as to where these differ from TCSEC B3. They have provided insight, and led to agreed interpretations, of the ITSEC requirements, particularly in the following areas:

a) Specification of semiformal security enforcing functionality in the security target: the evaluators identified a possible approach to satisfying this ITSEC requirement, which TIS has successfully applied in their security target for TMach.

b) Use of semiformal notation in the various design levels: an agreed interpretation has been reached, with TIS adopting their own notation at the architectural level, and using PDL with a design syntax and semantics at the lowest level. It was also established that the standard approach used in the Interface Specifications also qualified as a semiformal notation.

c) An agreement on the meaning of the term 'mechanism' used in various contexts throughout the ITSEC;

d) An agreed interpretation of the developer's security requirements has been reached: protection of the integrity of the target of evaluation (TOE) is the essential requirement, with protection of confidentiality aspects being a matter for the developer to decide.

These discussions and interpretations have had a significant impact on the development of the ITSEM and the Common Criteria.

Additionally, the evaluators have examined draft versions of the Security Administrator's Guide and Security Features User Guide: the initial assessment indicates that there should be no significant problems in satisfying the ITSEC E5 requirements in respect to Operation.

Finally, the evaluators have provided feedback on TIS's proposed approaches to addressing the ITSEC E5 effectiveness requirements. This discussion has served to clarify the ITSEC requirements, particularly in the areas of strength of mechanisms and binding analysis. The evaluators have also examined how the ITSEM approach to the evaluator's independent vulnerability analysis (which leads directly to penetration testing) should be applied on a full evaluation of TMach.

9. BENEFITS

The following benefits result from the TMach project:

9.1 Understanding the European approach on IT security evaluation

- The application of the European Criteria (ITSEC) to the evaluation of high assurance level (E5) has resulted in learning the strengths and weaknesses of the ITSEC.

- The ITSEC assurance effectiveness concepts which are somewhat different than the TCSEC approach are being applied in a high assurance evaluation which has resulted in clarification of concepts and shared understanding of approaches.

- The application of the ITSEC criteria has led to an increased understanding of the new concepts of:

  - separation of functionality and assurance
  - traceability
  - security target

- The evaluation process as described in the ITSEM has been applied which has resulted in significant shared understanding.

- The U.S. has gained understanding of the two most advanced European evaluation schemes (UK, Germany).

- Participating in the evaluation process has shown the procedures used within the UK and Germany for criteria interpretation.

- Answering questions of interpretation of various aspects of the ITSEC and ITSEM has actually helped to shape the criteria and processes.

- Dual evaluations of TMach with the UK and Germans in which meetings were held concurrently has resulted in significant communication between the UK and German evaluators and government officials. It appears that this has encouraged harmonization of processes within the two countries. Such harmonization makes the processes significantly easier for the U.S. to work with and understand.

9.2 Support of the development of new Criteria and U.S. Process

- The Common Criteria effort has profited significantly by the experiences gained within the TMach evaluation project.

- The U.S. development of the TTAP has been influenced by the experience of working with the European CLEFs.

9.3 TMach Analysis

- The TMach system has had the benefit of security analysis by a large collection of skilled evaluators. This will increase the confidence in the security of the system.

- Both the UK and German government officials have had the opportunity to learn about the TMach operating system which should improve its acceptability for use with their applications.