Doc Number N????

1003.22 Draft 2

Draft Guide for POSIX Open System Environment — A Security Framework

Sponsor

Portable Application Standards Committee
of the
IEEE Computer Society

Work Item Number: JTC x.xx.xx.x.x

Abstract: This standard defines a framework for security within the POSIX Open Systems Environment.

Keywords: Security, POSIX Framework, application portability, open systems,

1003.22 / D2
March 1994

ISBN 1-55937-061-0

Library of Congress Catalog Number 90-084554

Editor's Notes

This section will not appear in the final document. It is used for editorial comments concerning this draft.

This draft does not make full or correct use of the POSIX macros. This will be corrected in future versions as experience in their use is gained.

This draft has been prepared for submission to the IEEE Standards Review Committee.

Please report typographical errors (and index suggestions) to:

David Rogers
Data Logic Ltd.
Queens House
Kymberley Road
Harrow HA1 1YD
U.K.
+44 81 863 0383
FAX: +44 81 861 2010
E-MAIL: drogers@datlog.co.uk or d.rogers@xopen.co.uk

(Electronic mail is preferred.)

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of the IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, the IEEE and the members of its technical committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331

IEEE Standards documents are adopted by the Institute of Electrical and Electronics Engineers without regard to whether their adoption may involve patents on articles, materials, or processes. Such adoption does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the standards documents.

Contents

FIGURES

Introduction

(This Introduction is not a normative part of 1003.22 POSIX Open System Environment — A Security Framework, but is included for information only.)

Purpose

The purpose of this Guide is to define a generic security framework to provide a structured description of security within a POSIX Open System Environment that:

— identifies the security services required within an Open Systems Environment in support of portability and interoperability

— provides a framework that allows the implementation of different, user organisation specified information system security policies and security architectures. The system security architectures shall be those appropriate for single processor through to large, heterogeneous distributed system configurations

— describes the necessity for the deployment of varied security services and their how they are integrated to provide effective system security architectures

— assists in understanding the security relevance of Application Program Interfaces brought forward for standardization and help identify any enhancements or modifications required to adequately address security

— provide a basis against which the adequacy of the current implementations of security services may be compared

— provide a tool to help integrators of secure systems to understand and structure security services within a distributed system.

— provide a supplement to the definition of security currently included within POSIX.0 It is expected that this guide will be eventually be incorporated within, or referenced by, later issues of P1003.0.

Background

There is a wide range of threats and countermeasures that need to be considered when addressing the information security system needs. Currently, comprehensive and affective solutions employing many of the measures are either beyond available *commercial off the shelf* (COTS) technology or, if available, are not easily integrated to provide distributed system wide solutions. (The customised development of integrated security solutions cannot be cost justified by all but a few users.)

Most current standards provide little acknowledgement of security and security is generally inadequately addressed within them. The reason for this is that at the time such standards were prepared a general understanding of security, and the technical solutions available, were inadequately developed. Consequently it is not uncommon for application products to attempt to meet distributed system security requirements within their own domain of control. Consequently, different, and often non inetrworking and inadequate solutions to the same security requirements are devised and offered. the need is to provide a structured set of system security services, which are:

— deployed at the appropriate points in the distributed system architecture

— implemented by a minimum number of trusted components

— relied upon by the higher level application services to meet their security requirements

— easily managed

— scaleable to meet differing distributed system sizes and configurations.

Related Standards Activities

The following areas are under active consideration at this time, or are expected to become active in the near future for standards for application APIs that support the services defined in this guide. Similar efforts can be anticipated in the future [1]:

This section needs further consideration.

— POSIX.6 Security Extensions (Need latest title).

— Cryptographic Services

— Authentication and Related Services

— Portable Data Formats

— Network interface facilities

— System Administration

Extensions are approved as ‘‘supplements’’ or ‘‘revisions’’ to this document, following the IEEE Standards Procedures.

Approved supplements are published separately and distributed with orders from the IEEE for this document until the full document is reprinted and such supplements are incorporated in their proper positions.

---

1) A *Standards Status Report* that lists all current IEEE Computer Society standards projects is available from the IEEE Computer Society, 1730 Massachusetts Avenue NW, Washington, DC 20036-1903; Telephone: +1 202 371-0101; FAX: +1 202 728-9614. Working drafts of POSIX standards under development are also available from this office.

If you have any question about the completeness of your version, you may contact the IEEE Standards Department [+1 (908) 562-3800] to determine what supplements have been published.

If you have interest in participating in the working groups addressing these issues, please send your name, address, and phone number to the Secretary, IEEE Standards Board, Institute of Electrical and Electronics Engineers, Inc., P.O. Box 1331, 445 Hoes Lane, Piscataway, NJ 08855-1331, and ask to have this forwarded to the chairperson of the appropriate TCOS working group.

This standard was prepared by the P1003.6 Working Group, sponsored by the Technical Committee on Operating Systems and Operational Environments of the IEEE Computer Society. At the time this standard was approved, the membership of the P1003.6 Working Group was as follows:

Portable Application Standards Committee

Chair: Jehan-François Pâris

Standards Subcommittee for TCOS

Chair:
Treasurer:
Secretary:

P1224 Working Group Officials

Chair:	Lynne Ambuel (DoD)
Vice Chair (General):	Jon Spencer (Data General)
Vice Chair/Editor (Framework):	David Rogers (Data Logic)
Secretary:	David Ferbrache (Defence Research Agency)

Working Group

To be Completed.

The following persons were members of the P1003.22 Balloting Group that approved the standard for submission to the IEEE Standards Board:

To be added after final ballot.

When the IEEE Standards Board approved this standard on DATE it had the following membership:

(to be pasted in by IEEE)

Acknowledgments

TBA if required.