**Minutes of the distributed security study group meeting held on 11-15th January 1993 at the Hotel Intercontinental, New Orleans, USA.**

1. Sederunt

   David Rogers, Chair

   Manilal Daya
   David Ferbrache
   Piers McMahon
   Dick McNaney
   Lee Terrell

   The DSSG attendance list was circulated for updates and corrections.

2. Minutes of the previous meeting

   Noted that Richard Daugherty has been unable to continue as secretary due to work commitments. Agreed that Lee Terrell should contact Rich to obtain the draft minutes of the previous meeting. Agreed to start a new document register on the presumption of PAR approval.

   In the absence of these minutes the actions believed outstanding were reviewed, namely:

   > Update and release white paper: diagrams have been circulated for comment and note. The paper has been widely circulated for review, recipients include X/Open, DCE-Sig, IETF and TSIG.
   >
   > Draft and submit project authorization request: Noted that the chair has submitted a draft PAR to Jim Isaac for consideration by the PMC and SEC. This PAR is group document 003.

3. Liaison activities

   IETF: Piers McMahon reported that the access control group has been examining possible APIs. GSS API has been accepted for DCE 1.1 implementation.

   ISO: Agreed that Piers will review ISO's progress in the generic upper layer security work.

   X/Open: A copy of the white paper was available in time for the Munich X/Open meeting. Limited time was however available to discuss the contents at the meeting. Noted that X/Open security working group has undertaken two work items:

   > XDSF - X/Open distributed security framework - this activity is awaiting the outcome of the DSSG PAR approval process before proceeding. It is likely to the undertaken in close co-operation with the DSSG's activity.
   >
   > XMSF - X/Open minimum security functionality requirement - aimed at the definition of a set of minimum security requirements for X/Open systems. This work may have to be reconsidered in the light of the NIST/NSA Federal information processing standards activity.

   The security working group is pushing for inclusion of a security section in all X/Open documents. The DCE transaction processing group are considering incorporation of security functionality. Noted that X/Open is tracking the work of the DSSG towards the security framework.

   OSF: DSSG was represented at the December meeting in Cambridge. A great deal of interest was shown in the DSSG white paper, although questions regarding its direction were raised.

Noted that it was however the only attempt to document existing technologies within a common framework.

UNIX International: Noted that UI intends to establish a working group to address distributed system security. X/Open has contacted UI with a view to minimising duplication.

IEEE 802.10: Ann O'Neil has forwarded IEEE 802.10 draft 7 (Standard for inter-operable LAN security) which provides security at the link layer. The white paper has been copied to 802.10. Noted that both groups will meet in Denver, suggested that co-ordination be arranged. Consideration will be given to an afternoon joint meeting. Noted that 802.10 is due for publication in January 1993. Lee Terrell to review the standard on behalf of the DSSG.

EC Security investigations, project S2009: architectural guidelines: COMPOSITE: agreed to examine inter-relationship with framework document. Piers noted that the COMPOSITE activity does not attempt to draw separate architectures together into a common framework, but acts purely as a review of divergent architectures.

Federal criteria: noted that a revised draft is expected for public circulation in January. Noted that the DSSG is interested in receiving an advance copy for comment.

DRA technology demonstrator programme: agreed that David Ferbrache will circulate an abstract of the DRA's open distributed system technology demonstrator program for comment.

3. PAR approval

Noted that the PMC has approved the draft PAR. Agreed that the chair contact Roger Martin (sponsor for this PAR) to ascertain if any changes are required. The PAR is scheduled for discussion at the SEC on Thursday.

The proposed timescales for document production were noted: namely, first ballotable document by end January 1994, to complete ballot by end January 1995.

The contents of the draft PAR were reviewed. The inter-relationship with 1003.0 was considered. Agreed that the framework may eventually form an annex or appendix to the 1003.0 guide. The group was asked to delete references to closed standards groups such as OSF and UI in the liaison section. It was agreed that the review of existing applications form an informative annex rather than a substantive part of the guide. Agreed to add a reference to ISO/IEC JTC1/SC21/WG1 security framework standards activity.

Discussion have been held with the chair of POSIX 1003.6 concerning the inter-relationship between the two groups. Agreed that the group become a sub-group of the POSIX 1003.6 working group. The PAR was accepted by the SEC for forwarding to IEEE for final approval. SEC accepted the formation of a subgroup of 1003.6 to address this PAR.

The SEC requested that the chair consider the impact of the security framework on profile development.

4. Comments on the white paper

The group reviewed all comments received on the white paper. Agreed that the chair would respond to all personnel submitting comments with the groups views. The comments received form group document 004.

A general problem was encountered in the communication of the concept of security domains and the interaction of services via inter-domain services. This was complicated by the adoption of the ECMA terminology which was alien to the POSIX community. Agreed that additional effort must be expended on the clarity with which the domain concept is communicated, and that the terminology used in the body of the paper should be aligned to that of POSIX 1003.0 and .6.

The addition of a glossary of terms was agreed. Noted that the paper should not seek to comment on specific implementations of security functionality. The possible implementation of a component of the service security domain's security policy by the platform security domain was noted. Agreed to clarify the use of the work "privilege". Clarification of the concepts of "platform" and "co-operating process" are required.

5. First Joint meeting with 1003.6

   A joint meeting was held with 1003.6 to review the approach adopted by the white paper. The chair gave an overview of the history of the white paper. The following comments were noted:

   Section 1: noted that problems were encountered with clarity of text, particularly when not familiar with POSIX 1003.0 and ECMA TR-46 terminology and concepts. Requested inclusion of glossary, additional diagrams and examples. It was felt that "distributed" was a restrictive concept, the model being equally applicable to local security architectures.

   Section 4: the mapping of domains to administrative groups was queried. The generality of the adopted model was noted, and its possible extension to address non-security concerns noted.

   Section 5: to facilitate subject sponsor activities a concept of trusted path is required. The possible propagation of such trust via distributed trusted path was noted, along with the inherent problems of denial of service. Audit and security management must be addressed. The inclusion of trusted recovery functionality was considered. Agreed that the definition of data sets/ exchange formats for inter-operability was beneficial. This was considered to fall within the scope of POSIX standards activity. The possible inclusion of reliability and availability security functionality was queried.

6. Review of guide

   The group reviewed the structure of the guide to encompass the recommendations made by reviewers and 1003.6. It was agreed that its should mirror 1003.0 structuring, namely:

   1. Introduction: purpose, reference model, goals, benefits, related activities
      General: scope, normative references, conformance, test methods
      Terminology: conventions, definitions, abbreviations
   2. ECMA concepts
   3. POSIX 1003.0 open systems architecture overview
   4. Interpretation of ECMA security functionality in POSIX 1003.0 context
      structured into facilities, functionality, service API, data exchange formats

   Informative annexes:
   A. relationship to ISO frameworks and standards
   B. examples of interpretation for typical applications (email, multi-level db)
   C. review of existing industry practices
   D. how to use the guide
   E. mapping of organisation security policy

   + balloting instructions, bibliography, index

   The allocation of actions to group members was agreed, namely: David Rogers to revise section 2 and 4 to provide a mapping of the ECMA framework to 1003.0 (Chapter 2 & 4). Work on API and data exchange format definitions was deferred until the next revision has been completed. David Ferbrache to draft a glossary of terms. Lee Terrell to provide an overview of POSIX 1003.0 (Chapter 3). Piers McMahon to provide the text of annex A and annex D. David Ferbrache to consider possible application examples (annex B) and to examine the mapping of organisational security policies into the framework (annex E). The existing annex on industry practice will be extended to form annex C.

A February 26th deadline for redrafts was imposed to permit circulation and comment. Noted that the final version must be in the hands of the IEEE prior to the March 16th mailing deadline.

The general structure of the guide is to be revised to minimise assumed knowledge of ECMA and POSIX 1003.0. A clear mapping of ECMA concepts to POSIX 1003.0 facilities, from facility to security function, from function to service API, and from API to data exchange format is aimed for. Consideration of audit, security management functionality and of security implications of other POSIX 1003.0 service sets need to be undertaken.

7. Second Joint Meeting with 1003.6

A second meeting with 1003.6 was held to discuss co-ordination and future work.

Agreed that a study group be formed to address the PAR. This work would continue in parallel with other 1003.6 activities; namely ballot resolution on draft 13; new work in the areas of I&A, generic crypto interfaces, trusted path, portable data formats, administrative and network services. The security framework can serve as a planning and strategic document for 1003.6, providing not only a framework within which security services may be placed but also a means of identifying additional security functional areas for standards activity, and guiding 1003.6's work in the area of distributed security standardisation.

Agreed to re-organise the security functions section of the white papers to reflect areas of 1003.6 standards work, and to aim for adoption of common terminology. It was proposed that the SEC require standards to be reviewed against the security framework, and that appropriate consideration be given to security implications of work undertaken by other working groups. In this regard it was noted that 1003.6 has placed a priority on liaison activities with other standards groups.

8. Date of next meeting

The distributed security study group will meet as a sub-group of 1003.6 at Irvine, California in April 1993.

**Action Items**

| | |
|---|---|
| • contact Rich Daugherty to obtain the minutes of the previous meeting | Lee Terrell |
| • review 802.10 link layer security standard | Lee Terrell |
| • consider/review S2009 COMPOSITE and consider inter-relationship | Piers McMahon |
| • circulate TDP abstract to committee | David Ferbrache |
| • respond to comments received on white paper | David Rogers |
| • restructure white paper as detailed in item 6 | Study group |
| • forward PAR to NesCom for formal approval | David Rogers |
| • attend X/Open meeting Salt Lake City on behalf of DSSG | David Rogers |
| • mail .0 overview for incorporation in document | Lee Terrell |
| • consider impact of framework on profile development | David Rogers |
| • consider marketing of framework | David Rogers |

**Document register**

| | | |
|---|---|---|
| SD-001 | 1/93 | Attendance list |
| SD-002 | 1/93 | Email only members |

| | | | |
|---|---|---|---|
| 001 | 1/93 | Agenda, January 1993, Distributed security study group | David Ferbrache |
| 002 | 1/93 | Diagrams and illustrations for framework document | David Ferbrache |
| 003 | 1/93 | Draft PAR submitted to PMC | David Rogers |
| 004 | 1/93 | Comments received on the white paper | David Rogers |
| 005 | 11/92 | A distributed security framework for POSIX, issue 2 | DSSG |
| 006 | 1/93 | Revised PAR submitted to SEC | David Rogers |
| 007 | 1/93 | Revised chapter 3: interpretation of ECMA framework | David Rogers |
| 008 | 2/93 | Minutes of DSSG, January 1993 | David Ferbrache |