Copyright © 1991 by the
Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street
New York, NY 10017, USA
All rights reserved as an unpublished work.

This is an unapproved and unpublished IEEE Standards Draft, subject to change. The publication, distribution, or copying of this draft, as well as all derivative works based on this draft, is expressly prohibited except as set forth below.

Permission is hereby granted for IEEE Standards Committee participants to reproduce this document for purposes of IEEE standardization activities only, and subject to the restrictions contained herein.

Permission is hereby also granted for member bodies and technical committees of ISO and IEC to reproduce this document for purposes of developing a national position, subject to the restrictions contained herein.

Permission is hereby also granted to the preceding entities to make limited copies of this document in an electronic form only for the stated activities.

The following restrictions apply to reproducing or transmitting the document in any form: 1) all copies or portions thereof must identify the document's IEEE project number and draft number, and must be accompanied by this entire notice in a prominent location; 2) no portion of this document may be redistributed in any modified or abridged form without the prior approval of the IEEE Standards Department.

Other entities seeking permission to reproduce this document, or any portion thereof, for standardization or other activities, must contact the IEEE Standards Department for the appropriate license.

Use of information contained in this unapproved draft is at your own risk.

IEEE Standards Department
Copyright and Permissions
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA
+1 (908) 562-3800
+1 (908) 562-1571 [FAX]

5.2 System Security Services

Responsibility: Michelle Aden

5.2.1 Overview and Rationale

Information is the key to successful use of a system. For example, if used effectively and efficiently, information may be used to underpin enhanced service and to aid the derivation of strategic plans. Much of this information, for example, personal customer details and business financial plans, will be of a sensitive nature.

Although authorized users may be able to take advantage of the POSIX Open System Environment (OSE) to increase productivity and efficiency, unauthorized individuals may also be able to take advantage of the OSE to steal, manipulate or to deny others access to information held within the system, or to deny involvement in some transaction performed via the system.

Security services must therefore be provided within the system if it is to prevent these unauthorized activities. To achieve an optimum degree of confidence in the correctness and effectiveness of a system's security services, a system specific security policy must be derived and appropriate security functionality designed into the system at the beginning of its life cycle.

A relatively high degree of protection for ordinary computer systems can be achieved if system administrators correctly configure and maintain the system according to recommended security guidelines and practice, such as those described within the *X/Open Security Guide* . However, additional security facilities must be supported within the system to achieve protection against the small percentage of attackers who are noncasual, and who are determined to breach the security of the system. It is the intent of the security extensions to the base POSIX interface standard to support these additional security facilities.

The four basic security objectives of a system are to maintain:

— Confidentiality. The system must prevent unauthorized viewing of data.

— Integrity. The system must prevent unauthorized alteration or deletion of data.

— Availability. The system must ensure that authorized users are not prevented from accessing and processing data.

— Accountability. The system must ensure that users are made accountable for their actions, for example to ensure that users are correctly billed for system usage. See also 5.3.4.11. E

Different user groups may place different emphases upon these four basic security objectives. For example, the military security sector may place more importance upon confidentiality than accountability while, correspondingly, the commercial sector may place more importance upon accountability than confidentiality.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.2.2 Scope

One of the goals of system security is to provide defense in depth, such that if one layer of security is breached then further layers of security will limit and/or prevent unauthorized activities within the system.

To achieve a high degree of confidence in the correctness and effectiveness of the security of a system that will be processing sensitive information, security must be designed into the system at the beginning of its life cycle.

A System Security Policy (SSP) defines what it means for a specific system to be ''secure'' and, as such, forms the basic security input into the system lifecycle. Specification of an SSP is therefore axiomatic to the design of a secure system.

Although the SSP defines what security measures will be provided within the system, it is the system design documentation that defines how these security measures will actually be implemented.

One aspect of an SSP may be that it mandates conformance with the POSIX security extensions.

Security interface specifications are intended to assist in the construction of a secure system. They do not, in isolation, provide any protection against threats to a system. E

5.2.3 Reference Model

The reference model for security is the same as the model shown in Figure 3-3. E
Security has an impact on all of the APIs and EEIs in the model. E

5.2.4 Service Requirements

Through an analysis of the potential threats and requirements of the system, the system security objectives and hence the necessary System Security Policy (SSP) rules may be derived. This analysis must also take into account appropriate corporate, legal, and standardization requirements.

System confidentiality, integrity, availability, and accountability may be supported by the following security objectives:

Technical Security Objectives

— Identification and Authentication. A system entity, such as a user or system element, must prove that its claimed identity is legitimate, such that another system entity may place confidence in that claimed identity.

— Access Control. Access to system resources will be restricted to authorized entities only. Residual data contained within an object will be securely erased before it may be reused by a system entity.

— Accountability and Audit. System users must be made accountable for their actions. Audit trails of these actions will then be maintained and

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

utilized such that unauthorized system activity will be detected.

— Accuracy. The system must ensure that the correctness and consistency of security-relevant information is maintained.

— Availability. System resources will be provided to users in a consistent and reliable manner.

— Data Exchange. Data transmitted between system users and/or elements will be protected from unauthorized interference or viewing. Originators and recipients of data will be authenticated and will be able to mutually prove their respective participation in the transaction.

Nontechnical Security Objectives

— Assurance. The security of the system must be specified, designed, implemented, tested, and maintained in such a way that confidence can be placed in the correct and effective operation of the system. Also, procedures must be specified to ensure continued confidence in the security of the system in the event that the system is modified in some manner.

— Security Roles and Responsibilities. Security activities must be partitioned and allocated to identifiable security administrators who will then be responsible for ensuring that their allocated task is satisfactorily performed.

— Secure Operating Procedures. Procedures must be written that will guide system administrators and users as to the correct procedure to follow in the event of some security-relevant occurrence.

5.2.4.1 Application Programming Interface Services

E

The POSIX security interfaces will support Audit, Privilege, Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Information Labels (ILs). E

The audit services include: E

— Ability to record the user identification for actions within an audit trail E

— Ability to process the audit trail E

— Ability to use the audit trail to generate alarms E

The privilege control services include: E

— Ability to grant users only the minimal security required to perform a task E

This will minimize the impact of a subverted security administrator or unauthorized usage of a security administrator role. E E

The discretionary access controls (DAC) provide the following services: E

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

762 — Ability to control fine-grained user access to objects E

763 — Ability to provide extended user access bits beyond the traditional user- E
764 group-other E

765 — Ability to support access control lists (ACL) E

766 The mandatory access controls (MAC) and information labels (IL) support policies E
767 for labeling: E

768 — Ability to associate a MAC label with an object E

769 — Ability to label information (e.g., physical document handling restrictions) E

770 #### 5.2.4.2 External Environment Interface Services

771 *Note to reviewers: This subclause will be provided in a later draft. Mock ballot* E
772 *reviewers are welcome to submit comments on the types of services required at the* E
773 *EEI.* E

774 ### 5.2.5 Standards, Specifications, and Gaps

775 Table 5-2 lists the current, emerging, and gaps in security standards. E

776 **Table 5-2 – Security Standards** E

777

778

Service	Type	Specification	Subclause	E
779 System Security	E	IEEE P1003.6 API	5.2.5.2	E
780 Access Control	E	ISO/IEC 8613	5.2.5.2	E
781 Directory Authorization	S	CCITT X.509	5.2.5.1	E
782 Security	G	ECMA CMA 138	5.2.5.3	E
783 Trusted Systems	G	DOD 5200.28- STD	5.2.5.3	E

784

785 #### 5.2.5.1 Current Standards E

786 ISO 7498-2, *Information Processing Systems—Open Systems Interconnection Refer-* E
787 *ence Model, Security Architecture.* E

788 ISO/IEC 8613, *Information Technology—Text and Office Systems—Office Docu-* E
789 *ment Architecture (ODA) and Interchange Format.* E

790 CCITT X.509, *Message Handling System, ISO / CCITT X.400 Directory Authentica-* E
791 *tion Framework.* E

792 ECMA CMA 138, *Security In Open Systems—Data Elements and Service* E
793 *Definitions.* E

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.2.5.2 Emerging Standards

Information Retrieval, Transfer and Management For OSI —Draft Access Control Framework, ISO / IEC SC 21/ WG 1.

Draft Addendum to ISO 8613 On Security

The P1003.6 scope is limited to security extensions for those interfaces defined within the base POSIX interface specification (POSIX .1 {2}). Issues not addressed within the P1003.6 scope include noninterface-specific architectural assurance issues and communications security.

5.2.5.3 Gaps in Available Standards

The Information Technology Security Evaluation Criteria, Version 1.2, 28 June 1991.

US DoD, DOD 5200.28- STD, *Trusted Computer System Evaluation Criteria.*

Trusted Network Interpretation

Trusted Database Interpretation

Computer Security Subsystem Interpretation

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.3 Information System Management

Responsibility: Don Folland, Neil Croft

5.3.1 Overview and Rationale

Information System Management issues are considered in this clause. The subject is concerned with the effective management and control of the complete set of resources that comprise an information system. The tools in support of the services required by system managers need to reflect the portability and interworking attributes of open systems and fit the Open System Environment Reference Model (Figure 3-3). It is necessary to consider a variety of system management support scenarios (central management, dispersed management, or hybrid), addressing both distributed systems and standalone systems. The issues apply to application software or software components of the application platform. It is necessary to support automated management and operation of the IT infrastructure and address a wide variety of licensing scenarios. E

5.3.2 Scope

This category includes services and policies that address the administration of the overall information system required by any organization, including:

— Information Management

— Processor Management (e.g., Add new user)

— Network Management

— Configuration Management

— Security Management (e.g., Authentication, Key Management)

— Accounting Management

— Performance Management

Administration services accessible from the API may have Programming Language or Language Binding service specifications associated with them.

These services are defined to provide system and network administrator portability.

5.3.3 Reference Model

The Reference Model for system management is the same as the model shown in Figure 3-3. System management impacts all of the APIs and EEIs in the POSIX Open System Environment Reference Model. E

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.