-- --

# IEEE P1003.0 Draft 13 – September 1991

## 5.2 System Security Services

*Responsibility: Michelle Aden*

*HLJ : This is a complete clause replacement for Draft 13. It is not further diff-marked to avoid clutter.*

### 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* {*ref*}. 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.

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.

### 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.

The IEEE POSIX security group (P1003.6) has responsibility for defining the security extensions to the base POSIX interface standard. The POSIX 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.

### 5.2.3 Reference Model

The POSIX Reference Model partitions the Application Program Interface and the External Environment Interface into a collection of services, each one of which may have a security component. These individual components may operate independently or cooperatively with other security components. For example, a user identification and authentication operation may include elements of the User Interface Services, Communication Services, and Database Services.

### 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 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

**POSIX Security Interfaces**

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.

**POSIX Security Interfaces**

The POSIX security interfaces will support Audit, Privilege, Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Information Labels (ILs). Implementation support for these POSIX security interfaces is optional.

The audit interfaces support the concept of accountability wherein all system users are made accountable for their actions through the recording of user identities and associated actions within an audit trail. The audit interfaces support both portable audit generating and processing applications.

The privilege interfaces support the enforcement of a least privilege security policy wherein system administration responsibilities and associated privileges are allocated to a number of discrete roles, in order to compartmentalize the security impact of a subverted security administrator or of unauthorized usage of a security administrator role.

The DAC interfaces support the imposition of a fine granularity of user specified access control to objects. The DAC interfaces supplement the user-group-other permission bits that currently exist within the UNIX system through the use of Access Control Lists (ACLs).

The MAC and IL interfaces support the imposition of system specified policies for labeling. A MAC label is associated with an object (e.g., a file) and is typically used for access control purposes. An information label is associated with the data contained within the actual object itself and may therefore be used as a more accurate label for the purposes of hard copy printing. Further, an IL may contain information that is not related to logical access control and that is therefore not suitable for inclusion within a MAC label; e.g., physical document handling restrictions.

#### 5.2.4.2 External Environment Interface Services

*FGP: This subclause will contain the services from subclause 4.5.3 (supplied by POSIX. 6) that apply specifically to the API. For example, Access Control services will be in this collection.*

#### 5.2.4.3 Interapplication Software Entity Services

*FGP: This subclause will contain the services from subclause 4.5.3 (supplied by POSIX. 6) that apply specifically to the API. For example, Access Control services will be in this collection.*

#### 5.2.4.4 Component Management Services

*FGP: This subclause will contain the services from subclause 4.5.3 (supplied by POSIX. 6) that apply specifically to the API. For example, Access Control services will be in this collection.*

### 5.2.5 Standards, Specifications, and Gaps

#### 5.2.5.1 Related Standards in the POSIX OSE

ISO 7498-2, *Information Processing Systems—Open Systems Interconnection Reference Model, Security Architecture.*

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

*ISO / IEC 8613, Information Technology—Text and Office Systems—Office Document Architecture (ODA ) And Interchange Format.*

Draft Addendum to ISO 8613 On Security

CCITT X.509, *Message Handling System, ISO / CCITT X.400 Directory Authentication Framework.*

ECMA CMA 138, *Security In Open Systems—Data Elements And Service Definitions.*

*Card And Card Terminals, European Telecommunications Standards Institute, Terminal Equipment TE 9*

#### 5.2.5.2 Related Documents in the POSIX OSE

*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

#### 5.2.5.3 Emerging Standards in the POSIX OSE

To be provided.

#### 5.2.5.4 Related Standards

To be provided.

#### 5.2.5.5 Gaps in Available Standards

To be provided.

### 5.2.6 OSE Cross-Category Services

D

## 5.3 Information System Management

*Responsibility: Don Folland, Neil Croft* D

*DEF : The following is outline material as place-holder for more substantive text.*

### 5.3.1 Overview and Rationale

The following issues should be addressed in subclauses 5.3.1 and/or 5.3.2:

— should support a variety of system management support scenarios (central management, dispersed management, or hybrid)

— this section should address both distributed systems and standalone systems.

— could be applied to Application Software or software components of the application platform.

— support automated management and operation of the IT infrastructure

— should address a wide variety of licensing scenarios

### 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.