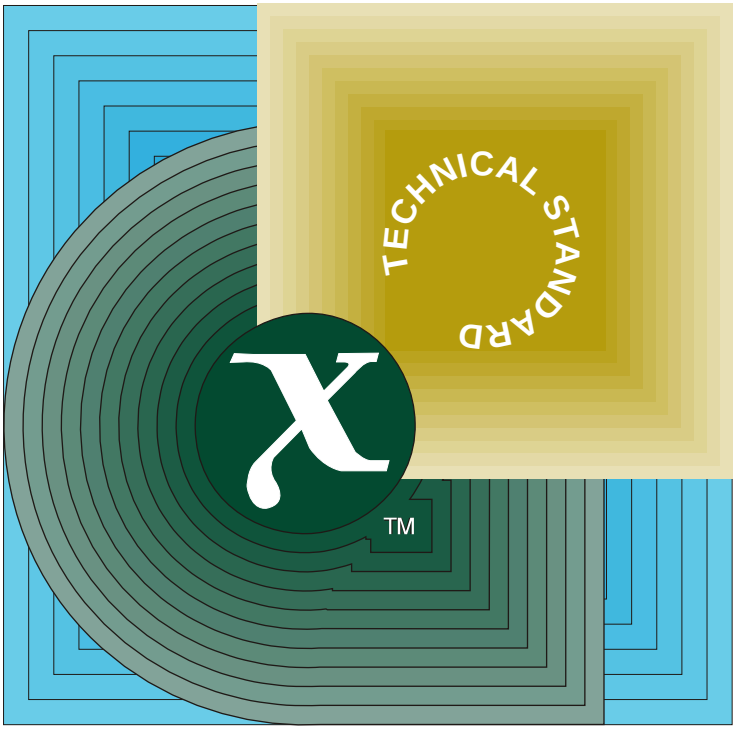
Technical Standard

X/Open Baseline Security Services (XBSS)



THE Open GROUP

[This page intentionally left blank]

X/Open CAE Specification

Baseline Security Services (XBSS)

X/Open Company Ltd.

X/Open CAE Specification

Baseline Security Services (XBSS)

ISBN: 1-85912-136-5

X/Open Document Number: C529

Published by X/Open Company Ltd., U.K.

Any comments relating to the material contained in this document may be submitted to X/Open at:

X/Open Company Limited
Apex Plaza
Forbury Road
Reading
Berkshire, RG1 1AX
United Kingdom

or by Electronic Mail to:

XoSpecs@xopen.org

Contents

List of Figures

List of Tables

Preface

X/Open

X/Open is an independent, worldwide, open systems organisation supported by most of the world's largest information systems suppliers, user organisations and software companies. Its mission is to bring to users greater value from computing, through the practical implementation of open systems.

X/Open's strategy for achieving this goal is to combine existing and emerging standards into a comprehensive, integrated, high-value and usable open system environment, called the Common Applications Environment (CAE). This environment covers the standards, above the hardware level, that are needed to support open systems. It provides for portability and interoperability of applications, and so protects investment in existing software while enabling additions and enhancements. It also allows users to move between systems with a minimum of retraining.

X/Open defines this CAE in a set of specifications which include an evolving portfolio of application programming interfaces (APIs) which significantly enhance portability of application programs at the source code level, along with definitions of and references to protocols and protocol profiles which significantly enhance the interoperability of applications and systems.

The X/Open CAE is implemented in real products and recognised by a distinctive trade mark — the X/Open brand — that is licensed by X/Open and may be used on products which have demonstrated their conformance.

X/Open Technical Publications

X/Open publishes a wide range of technical literature, the main part of which is focussed on specification development, but which also includes Guides, Snapshots, Technical Studies, Branding/Testing documents, industry surveys, and business titles.

There are two types of X/Open specification:

- *CAE Specifications*

  CAE (Common Applications Environment) specifications are the stable specifications that form the basis for X/Open-branded products. These specifications are intended to be used widely within the industry for product development and procurement purposes.

  Anyone developing products that implement an X/Open CAE specification can enjoy the benefits of a single, widely supported standard. In addition, they can demonstrate compliance with the majority of X/Open CAE specifications once these specifications are referenced in an X/Open component or profile definition and included in the X/Open branding programme.

  CAE specifications are published as soon as they are developed, not published to coincide with the launch of a particular X/Open brand. By making its specifications available in this way, X/Open makes it possible for conformant products to be developed as soon as is practicable, so enhancing the value of the X/Open brand as a procurement aid to users.

- *Preliminary Specifications*

  These specifications, which often address an emerging area of technology and consequently are not yet supported by multiple sources of stable conformant implementations, are released in a controlled manner for the purpose of validation through implementation of products. A Preliminary specification is not a draft specification. In fact, it is as stable as X/Open can make it, and on publication has gone through the same rigorous X/Open development and review procedures as a CAE specification.

  Preliminary specifications are analogous to the *trial-use* standards issued by formal standards organisations, and product development teams are encouraged to develop products on the basis of them. However, because of the nature of the technology that a Preliminary specification is addressing, it may be untried in multiple independent implementations, and may therefore change before being published as a CAE specification. There is always the intent to progress to a corresponding CAE specification, but the ability to do so depends on consensus among X/Open members. In all cases, any resulting CAE specification is made as upwards-compatible as possible. However, complete upwards-compatibility from the Preliminary to the CAE specification cannot be guaranteed.

In addition, X/Open publishes:

- *Guides*

  These provide information that X/Open believes is useful in the evaluation, procurement, development or management of open systems, particularly those that are X/Open-compliant. X/Open Guides are advisory, not normative, and should not be referenced for purposes of specifying or claiming X/Open conformance.

- *Technical Studies*

  X/Open Technical Studies present results of analyses performed by X/Open on subjects of interest in areas relevant to X/Open's Technical Programme. They are intended to communicate the findings to the outside world and, where appropriate, stimulate discussion and actions by other bodies and the industry in general.

- *Snapshots*

  These provide a mechanism for X/Open to disseminate information on its current direction and thinking, in advance of possible development of a Specification, Guide or Technical Study. The intention is to stimulate industry debate and prototyping, and solicit feedback. A Snapshot represents the interim results of an X/Open technical activity. Although at the time of its publication, there may be an intention to progress the activity towards publication of a Specification, Guide or Technical Study, X/Open is a consensus organisation, and makes no commitment regarding future development and further publication. Similarly, a Snapshot does not represent any commitment by X/Open members to develop any specific products.

Versions and Issues of Specifications

As with all *live* documents, CAE Specifications require revision, in this case as the subject technology develops and to align with emerging associated international standards. X/Open makes a distinction between revised specifications which are fully backward compatible and those which are not:

- a new *Version* indicates that this publication includes all the same (unchanged) definitive information from the previous publication of that title, but also includes extensions or additional information. As such, it *replaces* the previous publication.

- a new *Issue* does include changes to the definitive information contained in the previous publication of that title (and may also include extensions or additional information). As such, X/Open maintains *both* the previous and new issue as current publications.

Corrigenda

Most X/Open publications deal with technology at the leading edge of open systems development. Feedback from implementation experience gained from using these publications occasionally uncovers errors or inconsistencies. Significant errors or recommended solutions to reported problems are communicated by means of Corrigenda.

The reader of this document is advised to check periodically if any Corrigenda apply to this publication. This may be done in any one of the following ways:

- anonymous ftp to ftp.xopen.org
- ftpmail (see below)
- reference to the Corrigenda list in the latest X/Open Publications Price List.

To request Corrigenda information using ftpmail, send a message to ftpmail@xopen.org with the following four lines in the body of the message:

```
open
cd pub/Corrigenda
get index
quit
```

This will return the index of publications for which Corrigenda exist. Use the same email address to request a copy of the full corrigendum information following the email instructions.

This Document

This document is a *CAE Specification*. It represents the work of the X/Open Security Working Group and is intended to address limitations in the generic security features of open systems.

This document is structured as follows:

- Chapter 1 is an introduction to the concept of the X/Open Baseline Security Services (XBSS) specification and its implications to Security Branding.
- Chapter 2 explains the way in which the XBSS addresses the security needs of the business community.
- Chapter 3 is an overview of the security functionality statements and the rationale for selecting the features described.
- Chapter 4 is a detailed description of each functionality statement and the default value accompanying it. This chapter contains the normative statements of functionality that are the core of the XBSS.
- Appendix A is a description of the generic X/Open Branding Procedure.
- Appendix B compares the security functionality of the XBSS with other popular profiles. It provides a more detailed discussion of ideas introduced in Chapter 3.
- Appendix C discusses the reasons why certain security functionality is not currently within the scope of the XBSS, explains what work is in progress, and gives suggestions and pointers on how systems might be made secure in the absence of international standards.

- Appendix D provides the names of companies and organisations associated with the development and review of the XBSS.
- Appendix E gives detailed explanations on the use of some terms and includes a standard glossary.

Intended Audience

The X/Open Baseline Security Services (XBSS) specification is targeted at security specialists who provide technical guidance to :

- product procurers, with respect to security functionality required to support their installation's security policy
- product suppliers, with respect to security functionality required by their products to support baseline security policies of XPG4 compliant and Single UNIX Specification compliant systems.

It is helpful if these persons are familiar with any of the following:

- the security functionality of the US Department of Defense Trusted Systems Evaluation Criteria (TCSEC) C2 level
- the Information Technology Security Evaluation Criteria (ITSEC) F-C2 sample functionality class
- the Minimum Security Functionality Requirements (MSFR)
- the Federal Criteria or Common Criteria concept of Protection Profiles (PPs) and their sample protection profiles for commercial systems CS1 and CS2.

Trade Marks

UNIX® is a registered trade mark in the United States and other countries, licensed exclusively through X/Open Company Limited.

X/Open® is a registered trade mark, and the ‘‘X’’ device is a trade mark, of X/Open Company Limited.

Acknowledgements

X/Open acknowledges the co-operation of the European Security Forum (ESF) and the contribution of members of the Forum's UNIX Special Interest Group. Alan Stanley and Marco Kapp were the project leaders of this work.

The full membership list for the ESF (for November 1995) is given in Appendix D.

Appendix D also lists the companies and organisations which are represented on the X/Open XBSS Project Group and on the X/Open Security Requirements Topic Group.

Referenced Documents

The following documents are referenced in this document:

Bellcore Requirements
: Bellcore Standard Operating Environment Security Requirements. Technical Advisory TA-STS-001080, Issue 2, June 1991

Business Requirements for Upgrading UNIX Security
: Published February 1995 by the European Security Forum

Common Criteria
: Common Criteria Editorial Board, Draft Common Criteria for Information Technology Security Evaluation,Version 0.6, CCEB-94/041, April 1994. (The Editorial Board consists of members from the CSE DGI, EC DGXIII/B, U.S.A. NIST and U.S.A. NSA)

CISR
: I-4, Commercial International Security Requirements (CISR) Cutler/Jones Draft Revision January 1991

COFC
: Standard ECMA — 205 Security Oriented Functionality Class (COFC) for Security Evaluation. December 1993

FC
: NIST/NSA, Federal Criteria for Information Technology Security Version 1.0, December 1992

IEEE
: IEEE Std. 1003.3-119, IEEE Standard for Information Technology — Test Methods for Measuring Conformance to POSIX

Information Technology — Code of practice for information security management
: ISO/IEC DIS 14980. Published by the International Organisation for Standardisation. This document is based on the U.K. Department of Trade's publication BS7799 ''Code of Practice for Information Security Management''

MSFR
: NIST, Minimum Security Functionality Requirements (MSFR) for Multi-user Operating Systems. Issue 2, August 1992

NCSC-TG-023
: NIST, NCSC-TG-023, A Guide to Understanding Security Testing and Documentation in Trusted Systems, July 1993

Practical UNIX Security, 2nd edition
: Garfinkel and Spafford, published by O'Reilly & Associates, Inc. June, 1993.

Security Guide, 2nd edition
: Published by X/Open. Document number G010

TCSEC
: Trusted Computer System Evaluation Criteria. U.S. Department of Defense (DOD), 1985 DOD 5200.28-STD, National Computer Security Center, Fort Meade, Md. (also known as the Orange Book).

Chapter 1

Introduction

This chapter provides an overview of the X/Open Baseline Security Services (XBSS).

It provides a high-level description of the XBSS, explains why it has been developed, who it is aimed at and its scope.

1.1 What is the XBSS?

The XBSS presently consists of a specification covering:

- a *base* set of security-related functionality to be provided by Open Systems
- the *default settings* of security-related parameters associated with such systems.

The XBSS is a *Protection Profile* (see Section 3.2 on page 11) with only the Security Functionality component defined.

The XBSS is intended to be used as part of an X/Open branding programme (see Appendix A on page 47) for the branding of systems that guarantee to support security as defined in this specification.

1.2 Why the XBSS has been Developed

The XBSS has been developed to provide buyers of X/Open-branded systems with assurance that such systems provide a defined minimum level of protection, consistent with accepted good practice and capable of meeting key business needs in a cost-effective fashion.

1.3 Market Focus

The XBSS addresses the concerns and priorities of private and public-users of open systems who need assurance that such systems are capable of providing a reasonable level of protection against the sorts of disruptive events which commonly occur in the world of business and public administration, such as accidents, errors, unauthorised use and amateur but malicious tinkering.

It is not intended to provide a solution for applications involving highly-classified information in military or other governmental environment, or in situations where attacks are concerted and malicious and take advantage of obscure and little known design flaws using innovative techniques that are one step ahead of protection mechanisms.

1.4 Technical Scope

1.4.1 Degree of Interworking

In dialogues with the X/Open Security Requirements Topic Group (SecRTG), three potential scopes were discussed:

- stand-alone
- interconnected homogeneous
- distributed heterogeneous.

(An explanation on the meaning of these terms is provided in Appendix E on page 69)

The XBSS occupies an environment which is shown in graphic form in Figure 1-1.

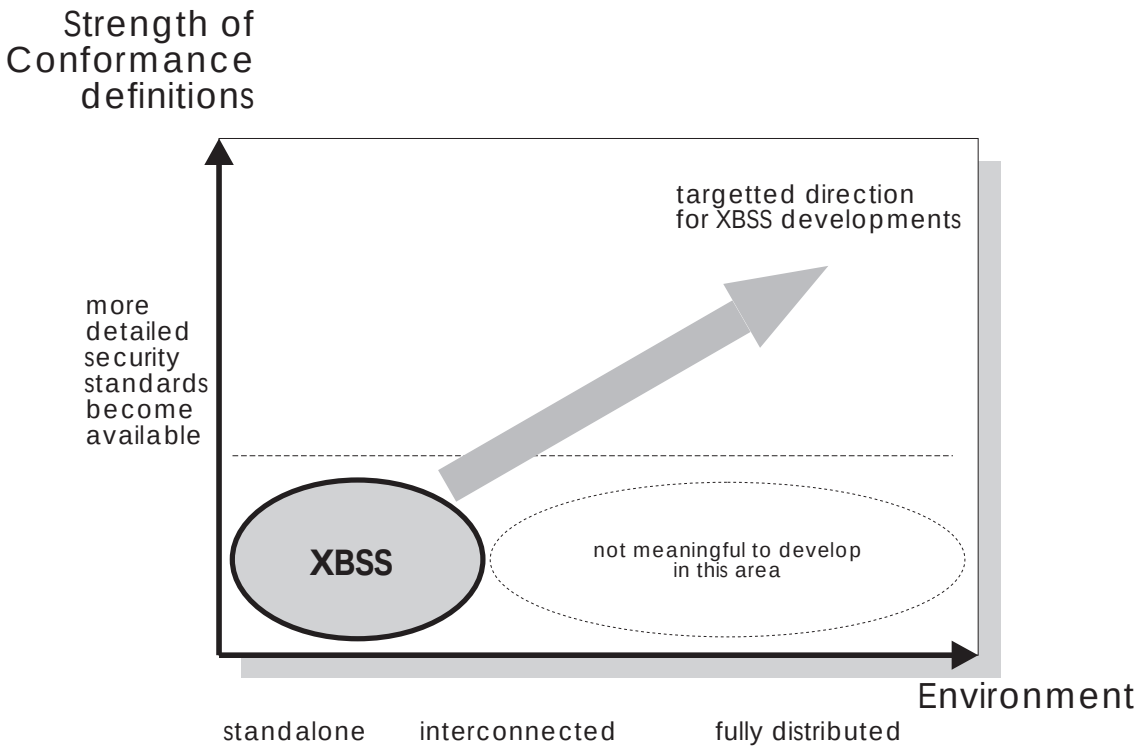


Figure 1-1 Intended Development Path for the XBSS

The XBSS currently sets a standard for system in a stand-alone environment. By making use of detailed security service specifications for APIs, protocols and data formats, the XBSS will progress along the development path indicated, adding at each stage more detail to the conformance requirements for security functionality.

The target is a future XBSS which is supported by strong conformance definitions derived from solid, internationally-agreed standards, and which allows the XBSS to address the interconnected and ultimately the distributed computing environment.

The scope statement for the XBSS can be expanded as follows:

- Although primarily focused on open systems, the XBSS is applicable to the full range of offerings carrying the X/Open brand and, in principle, to *other* multi-user operating systems.
- The intention is that the XBSS should be introduced in such a way that upgraded products can be brought to market quickly. XBSS specifically does not include requirements for distributed security services at this stage but this does not preclude the XBSS-Branding of interconnected systems. The objective is to address the issue of *heterogeneous systems* (i.e., interconnected systems of varying types) as soon as possible in a future issue of the XBSS.

1.5 Development Process

The XBSS has been developed in response to requirements identified in 1991/92 by the X/Open Xtra process for establishing market needs.

Development has been led by the X/Open Security Working Group, with valuable input from over one hundred companies in the public and private sectors, including members of the X/Open User Council and X/Open Security Requirements Topic Group, and from the European Security Forum. A full list of the organisations involved is supplied in the acknowledgements section at the beginning of this document.

The XBSS development process featured four main elements:

- Existing checklists of security requirements were examined and used to construct a comprehensive, composite schedule of detailed security requirements. This was circulated in draft for constructive criticism by a wide range of commercial organisations and other institutions.
- The most urgent and important business requirements for upgrading open systems security were identified in conjunction with leading businesses. This phase of activity involved members of X/Open Company's User Council and Requirements Topic Group with special input from the European Security Forum.
- Suppliers represented on X/Open Company's Security Working Group and user organisations worked together to arrive at a pragmatic judgement about which requirements should be featured in the initial XBSS specification, balancing the need for significant improvements in the security of open systems against resource availability and the desire for upgraded products to be available quickly.
- The XBSS specification is intended to support branding of security related products under the X/Open Brand.

Together these arrangements give a high degree of confidence that the XBSS addresses key business needs in a realistic manner, to the benefit of buyers and suppliers of open systems.

1.6 How to Interpret the Remainder of this Document

The **Structure** section of the *Preface* of this document briefly explained the content of the chapters and appendices.

Chapter 4 on page 17 lists the security functionality which comprises the XBSS. The bulleted statements, printed in **bold type**, represent the minimum functionality that a vendor must provide in order to produce a system that is capable of being X/Open Security Branded (subject to additional X/Open Branding requirements, see Appendix A).

Chapter 4 satisfies, in part, the business requirements for a secure open system. However, not all the business needs can be met at the present time. Appendix C on page 61 discusses the reasons why certain security functionality is not currently within the scope of the XBSS, explains what work is in progress, and gives suggestions and pointers on how systems might be made secure in the absence of international standards.

When considered together, Appendix C and Chapter 4 go a very long way to addressing the security problems in open systems which businesses have today.

X/Open understands and accepts the problems which business users face and the requirements that they wish to see implemented. Appendix C states those requirements which can be addressed within the scope of X/Open work and points to work in progress which will result in specifications in the future. It also explains X/Open Company's position on the secure networking requirement.

Chapter 2

Business Needs

2.1 Purpose

The purpose of the XBSS is to indicate to users that the initial settings of a branded computer system will provide a best practice profile of security functions and settings. It is to indicate that if you buy an X/Open branded system, then the organisation can have a level of confidence that the systems will work safely.

This is particularly relevant as organisations become increasingly distributed and resources for managing systems is reduced. Business users will have to accept responsibility for the management of their systems and, without the specific skills to determine the security settings, more reliance is placed on the specification of systems.

2.2 Scope

This is essentially a technical document and provides much detail on the particular security services and their associated default settings. These services have been selected by security professionals with regard to best practice. Readers may wish to confirm the range of security services implemented by referring to the later sections contained in this specification, but by buying a branded system, they can have confidence that the system is secured to the defined level of good security practice. This chapter explains how the XBSS addresses the security needs of the business community. It sets the scene by presenting a business view of information security and the particular challenges associated with the security of open systems.

Key business requirements are then defined along with the benefits of satisfying these requirements. Finally the business community's support for a commercially-driven approach to security branding is discussed.

2.3 Constraints

This specification will develop as Figure 1-1 on page 2 has illustrated. Additional security requirements will be identified and the XBSS will change in a series of steps, each building on the work that has gone before. Branded products will be associated with particular versions of this specification. Undisclosed functionality is not explicitly addressed, but vendors will be required to undertake due diligence so that organisations can be confident that products provide a reasonable level of confidence that the product has no undisclosed functionality.

2.4 Business View of Information Security

Throughout the last decade, companies and public sector bodies have continued to invest heavily in computer and network systems. In a fiercely competitive world, investment is set to continue as organisations of all types and sizes strive to reduce their costs and give value-added services to customers.

As these organisations become more dependent on computer-based information systems, management has become increasingly aware of the need to protect the ability of their organisation to function in the event of a failure in the confidentiality, integrity and availability of their corporate systems and the data held therein.

The dual threat is:

- **deliberate abuse** such as theft of computer equipment, falsification of data, sabotage of systems and data, and improper use of corporate computers and networks by unauthorised users
- **accidents and errors** which can compromise the availability, integrity or confidentiality of corporate information. Besides those accidents traditionally classed as ''acts of God'' there are the more common occurrences of software and hardware malfunction, programming and user errors, and unforeseen effects, including the inability of a system to cope with peak or unexpected loading.

While much publicity and attention has been devoted to the deliberate abuse of computer systems, there is evidence that most losses suffered by commercial organisations are due to accidents or errors rather than to hostile attack.

There is a business need to protect corporate systems from the sorts of accidents and mistakes encountered in the daily operation of the system, and this should be done in an efficient and cost-effective manner.

2.5 Security of Open Systems

Much of the business community's investment in computers and networks is centred on *open* systems and there are particular challenges to be addressed in securing such systems.

Though many systems now carry an open systems label, some of which bear the X/Open Brand, in many people's minds open systems tend to be UNIX systems. The UNIX system originated in research and academic environments where security needs are different from those in the business sector. The commercial world has long held reservations about the security which the UNIX system offers and has often sought to enhance system security at some expense, using system experts to graft security functionality onto UNIX systems, forming highly secure installations in the process.

This is not a satisfactory solution to the general problem. Very few commercial organisations have either the capability or desire to write security code for their systems; neither do they wish to buy the specially secure versions of the UNIX system presently on the market.

The UNIX system is one of the main operating systems of choice in the commercial world and it is therefore important that the system suppliers address this problem of security.

2.6 Key Business Requirements

The business community's reservations about UNIX system security need to be addressed in a generally-applicable manner, which can be of use to businesses ranging from the very small to the very large.

2.6.1 Work of the European Security Forum (ESF)

Work done by the European Security Forum has identified 15 specific business requirements for upgrading the security of UNIX system. These requirements can most easily be presented in three groups, as follows:

- **Group 1 Minimising Intervention**: this first group of requirements addresses the business need for systems which can be secured easily and cheaply — in many cases with minimal extra intervention. The key business requirements in this group are:
  - — *Secure Running on Delivery* (specifically, suppliers to set sensible defaults for security-related parameters)
  - — *Simplification of Installation, Administration and Operation*
- **Group 2 Enhancing Security Functionality**: this second group of requirements covers the security-related functionality in most urgent need of improvement, in the field of open systems. The key business requirements in this group are:
  - — *Control of Access Privileges*
  - — *Secure Networking*
  - — *Secure Audit Trails*
  - — *Single Logon*
  - — *Unique User Identities*
  - — *Secure System Inter-operability*
  - — *Improved Backup and Recovery*
  - — *Improved Error Avoidance and Recovery*
  - — *Improved File and Record Locking*
- **Group 3 Key Constraints**: this final group of requirements sets some conditions to be satisfied in upgrading the security of open systems. The key business requirements in this group are:
  - — *Greater Standardisation*
  - — *Impact of Security on Performance* (specifically, suppliers should ensure their products provide acceptable performance when security features are turned *on*)
  - — *Avoidance of 3rd-party 'Freeware'*
  - — *Single-point of Supply for Base System and Add-ons*

Together these 15 business requirements represent a realistic agenda for action by the open systems community. They directly address the need for a balanced approach to the categories of threat most commonly encountered in business life, and the need for security solutions which can be implemented in practice in most, if not all, businesses.

2.6.2 The U.K. Department of Industry (DTI) Code of Practice

The X/Open Security Requirements Topic Group have noted a close congruence between the XBSS and the DTI Code of Practice. They conclude that the XBSS does support the Code of Practice[1] to the degree to which it is able at present and that future developments in the XBSS will lead to a closer mapping.

2.7 Business Case for Upgrading the Security of Open Systems

Any approach to upgrading the security of open systems must be seen as realistic from the perspective of both buyers and suppliers of such systems.

2.7.1 Benefits to Buyers

The indications are that satisfying the business needs identified in Section 2.6 above will be of considerable benefit to buyers. In particular buyers should benefit from reductions in the:

- need for costly countermeasures
- lifetime cost of ownership of open systems
- overall risk of ownership of open systems.

2.7.2 Benefits to Suppliers

Suppliers will be able to obtain a significant return on their investment in upgrading their open systems in the security arena. Upgrading to satisfy the business needs identified in Section 2.6 should:

- help suppliers keep their products competitive in the face of emerging proprietary alternatives
- allow suppliers to charge realistic prices for enhanced products
- lead to increased sales: Software houses will see cost and time-saving advantages in developing packages for those open systems which have upgraded security at operating system level. This in turn will lead to the a wider acceptance of open systems in corporate purchasing. In a recent survey[2] one in five businesses reported that restrictions were imposed on the choice of systems which they could consider for purchase.

---

1. See also Section C.1.1 on page 61.
2. See ''Business Requirements for Upgrading UNIX Security'' in the Referenced Documents section at the beginning of this document.

2.8 Demand for a Commercially-driven Approach to Security Branding

The survey results contained in ‘‘Business Requirements for Upgrading UNIX Security’’ show that there is very strong support amongst leading organisations for a security brand provided by the commercial world rather than by governments.

It also shows there is widespread demand for security requirements and priorities to be defined by the commercial community (i.e., the private sector), and for standards to be developed by an independent body supported by the business community, rather than by a government-controlled body. This view is held by public sector institutions and companies alike.

There is evidence that most businesses are looking for a commercial security brand. The advantage of a commercial security brand is that it:

- addresses procedural issues as well as technical requirements
- provides practical improvements to the problems associated with system administration, in the absence of a complete solution
- will mandate standardised interfaces, a given set of security functionality, and will encourage a common look-and-feel
- enables a supplier to warrant conformance without being subjected to a lengthy, formal, third party evaluation
- will provide some form of sanction against suppliers making unjustified claims as to the compliance of their X/Open branded product.

The points above are strongly supported by the survey, which was carried out with the active support of X/Open. The survey results as a whole provide a powerful support for the main elements of the XBSS proposal.

Chapter 3

Relationship to Evaluation Criteria

3.1 Introduction

Security Branding using the XBSS specification is X/Open Company's response to the business community's demand for a commercially-driven approach to the security evaluation of open systems. However the body of knowledge, experience and technology on the subject of secure or trusted systems has accumulated as the result of a decade of evaluations using various government-sponsored national and international programmes.

The XBSS cannot ignore this mass of knowledge, rather it must show how it has built upon it, using the perspective and requirements of the commercial market.

Furthermore, for any commercially driven approach to gain the support of the established evaluation community, it must be defined in terms familiar to that community.

The following sections explain how the XBSS has been derived directly from the foregoing programmes and how it can be thought of in terms of the established technology.

3.2 The Protection Profile

A protection profile (PP) is an abstract, product-independent specification of the security aspects of an Information Technology product. It is a concept introduced by the U.S. *Federal Criteria* (refer to Federal Criteria document). The specification binds together requirements for protection functions and assurances, with rationale describing the anticipated threats and intended method of use. The security functions and assurances are assembled from predefined generic functional and assurance components, but the creator of the protection profile is expected to interpret these generic requirements for the target usage environment. Interpretation may be comprised of the assignment of specific constants, authorisation rules or specific conditions, and it may include the refinement of specific requirements. An important principle of Protection Profiles is that the building block sub-sections should not be reproduced verbatim, rather they should be interpreted by expert representatives of the target market and that they be elaborated upon so that no ambiguity or need for further interpretation remains. Sample commercial profiles, such as CS-2 and CS-3, supplied with the Federal Criteria, theoretically provide commercial systems with enhanced protection against increasingly serious and more subtle security threats, but they have not been shown to represent the needs of a particular market sector or product base. X/Open has tailored a protection profile of baseline security functionality specifically to address the needs of the open commercial market that it understands very well. X/Open has used the model suggested by the Federal Criteria document but not the sample commercial profiles, CS-2 or CS-3, because they do not match the baseline security requirements as understood by X/Open.

3.2.1 Rated Functional Component

A rated functional component is a set of rated requirements for protection functions to be implemented in an IT product. Being rated means that the functional component has a hierarchical set of increasingly protective and comprehensive capabilities. For example the Access Control functional component has four rated levels, AC-1, AC-2, AC-3 and AC-4. AC-1 is considered minimal, AC-2 basic, AC-3 extended and AC-4 fine-grained.

3.2.2 Functional Component Primitive

Each functional component may consist of one or more separate functional requirements called primitives. Thus AC-1 includes a list of five primitives including the requirements for access control attributes, administration of those attributes, authorisation of object references, creation and destruction of subjects and objects, and finally object encapsulation.

3.2.3 Why X/Open Created a New Protection Profile

Considerable effort and expertise has gone into the creation of sets of commercial security functionality requirements. Most notably the Minimum Security Functionality Requirements (MSFR) was distributed as a draft US National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS). This FIPS was the result of combined inputs from Bellcore, from NIST and from the Commercial International Security Requirements (CISR) of the International Information Integrity Institute (I-4).

The European Computer Manufacturer's Association (ECMA) used the MSFR to derive the Commercial Oriented Functionality Class (COFC), which became an ECMA standard for use as a functionality class in ITSEC evaluations.

More recently, the Federal Criteria introduced a sample set of Protection Profiles for use with commercial systems was introduced into the Federal Criteria. The first, CS-1 corresponds to the TCSEC C2 functional and assurance requirements, while CS-2 and CS-3 represent increasingly stringent sets of security functionality and assurances designed to support increasingly protective commercial security policies.

In compiling the XBSS functionality component, X/Open studied the above sources, in depth, and reached the following conclusions:

- The rated functional components of the *Federal Criteria* represent the most advanced and comprehensive set of security functionality primitives. These components incorporate the MSFR which as a result was not issued as a formal FIPS. These functional components represent an advance on the "state of the art" as represented, for example, by the System Entry and System Management components.
- The *Federal Criteria* functional components are presented in a hierarchical format, thereby allowing X/Open to select from higher levels in this hierarchy as it evolves the security functionality specifications.
- The MSFR is seen as a set of security functionality that represents the commercial users view of the complete ideal. As such, it is a target for suppliers to aim at and more of the MSFR derived requirements may be added to the XBSS at a later date. In practice, the need for early acceptance constrains the selection of functionality to that which can be reasonably implemented by suppliers within 1 year of publication of the XBSS CAE specification.
- The *Federal Criteria* concept of Protection Profiles, which is being carried over into the Common Criteria, is ideally suited to the objective of X/Open to address the security needs of the XPG4 Base Definition Profile and the XPG4 UNIX Profile Definition. Since the protection profile concept calls for the unambiguous interpretation of the rated functional

component primitives for selected market segments, this seems to fit well with the need to tailor security functionality requirements to X/Open CAE components.

- The *Federal Criteria* sample protection profiles were all unsuitable. CS-1, by being constrained to correspond to the TCSEC C2 requirements, is now seen to be less than minimal. By contrast CS-2 and CS-3 were found to be more than baseline in many functional areas. For details read the rationale section in Appendix B or for a summary comparison study the table, Table B-1 on page 58 and its associated text.
- The COFC was found to be unsuitable as a basis for the XBSS because in many requirement areas it represents a generalisation or simplification of the MSFR. Whereas the Federal Criteria protection profile allows for interpretation of generic primitives, the COFC leaves too much for interpretation by the supplier. X/Open does however agree that the implementation of lower level security mechanisms should be left to the suppliers.

3.3 X/Open Baseline Security Services

The XBSS is the protection profile chosen for the open systems commercial market. It consists of a set of rated functional components, chosen from the set of generic rated components defined in the Federal Criteria and is patterned after the sample commercial protection profiles, CS1, CS2 and CS3, defined in Volume II of the Federal Criteria. In line with those examples, the generic functionality requirements have been interpreted and refined for the open systems market (see Section 7.2 of the Federal Criteria).

The rationale for the choice of components is given in Appendix B. A comparison of the XBSS with CS-1 through CS-3 is presented in the table in that appendix.

This profile is a starting point for what is expected to be an evolving process. The profile is expected to evolve in several directions:

- Regarding system architecture, it will start by addressing interconnected homogeneous systems and will evolve to heterogeneous distributed systems.
- Regarding the depth of coverage of security functionality, as common standards for security functionality are developed, the XBSS will evolve to take advantage of them. For instance, the XBSS may in future state that not only must a particular piece of functionality exhibit a defined list of capabilities and behaviour, but that it must also be supplied through specific application programming interfaces (APIs), protocols, and data formats.

The XBSS has been defined by the X/Open Security Working Group (SWG) as a result of requirements received from the X/Open User Council and has been identified by various consultants and organisations as being most appropriate for the existing commercial open systems market.

3.4 Defining the Target of Conformance

One problem of evaluations also applies to an X/Open security brand. What product, set or subset of products should be the target of branding? A vendor may have a packaged product consisting of an operating system, subsystems and applications, ready to be loaded and used by their customers. Yet that vendor may realise that only a certain subset of the package can meet the requirements of the specification. It is not practical for X/Open to predefine exactly what should be submitted for branding; this must be left up to the vendor. Therefore one of the first entries to be made in the *Conformance Statement* is the vendor definition of the *Target Of Conformance* (TOC). This is a similar concept to the *Target Of Evaluation* (TOE) introduced by the ITSEC, and as with such an evaluation programme, the vendor must state that any products, subsystems or applications added to the TOC may change the security characteristics of the branded system with unknown results.

3.4.1 Target of Conformance and Hardware Platforms

Although every target of conformance must include a hardware platform (certain security functions depend upon hardware to implement such things as memory management, separation of processes, and so forth) it is not the intention of this specification to require specific hardware functionality. This allows suppliers to specify components as conformant irrespective of the hardware platform. All that the conformance requires is that the hardware platform provide the necessary support to enable the required software security functionality.

3.4.2 Target of Conformance and Trusted Computing Base (TCB)

The TCSEC or Orange Book (see Referenced Documents) defines a TCB as the totality of protection mechanisms, including hardware, firmware and software, that together enforce a security policy.

The security functionality requirements listed in Chapter 4 use the term TCB, because, like the TCSEC, the XBSS specifies security functionality requirements needed to enforce security policy, but without explicit hardware or firmware requirements, even though they may be implicit for certain mechanisms.

Since a supplier claiming conformance may include software that contains no security relevant code, the TOC may be greater than or equal to the TCB, but never smaller than the TCB. This latter claim assumes that all security relevant code must contribute in some way to a security policy and must therefore be part of the TCB.

3.4.3 Making Changes to the Target of Conformance (TOC)

It may be possible for a user to add-on or modify the TOC such that conformance may be compromised. The vendor is required to provide criteria to discriminate between applications that may compromise conformance and those that can be safely added to the TOC without compromising conformance — see Section 4.10.2 on page 44.

3.4.4 Claiming Conformance for Add-on Sub-systems

Third-party products may at times be combined with another vendor's base products in order to give added value to the customer.

This combination can constitute the Target of Conformance (TOC) when registering a product for the X/Open Brand.

Either the base provider or the third-party product provider can apply to register the new TOC.

3.5 Assurance Requirements

The assurance requirements provided by the XBSS are not the same as those defined in the Federal Criteria for protection profiles. The vendor will provide a guarantee of conformance by a number of means:

- The X/Open Brand.

  The vendor warrants and represents that his product complies with the XBSS. The vendor thereby states that the required functionality has been established and the product works and will continue to work. If a non-conformance is later found, the problem will either be addressed within a specified minimum timeframe or the vendor will lose the X/Open Brand.

- The publicly available Conformance Statement.

- The claim of comprehensive testing that indicates that the required security functionality works as specified in the XBSS specification and as documented in the vendor-supplied user and administrator's guide.

Chapter 4

Functionality Detail

This chapter provides detailed requirements for the seven functional components required for the XBSS. For each functional component, the security functionality primitives are defined in the context of the XPG4 Base environment, with notes and comments provided to illuminate the meaning of the requirement and suggestions as to the benefits accruing from an implementation of the requirement.

4.1 Normative Text

Only the items contained in the sub-section **Requirement Detail** are normative. The wording is precise, and many terms have glossary entries. Some terms, such as TCB (Trusted Computing Base), have already been defined (for TCB see Section 3.4.2) but other special terms (e.g., ‘‘protected mechanism’’) and words used in special ways (e.g., ‘‘normal user’’) are defined in Appendix E on page 69.

The normative text is in a **bold typeface**.

The text in the sub-section **Description and Rationale** is not normative. This is the notes and comments text.

4.2 The Default Parameters for the XBSS

Where appropriate the default settings are given. The XBSS requires that the product be shipped with secure default settings predetermined by the vendor (the vendor defaults).

These defaults are normative and are printed in an ***bold italic typeface***.

The purpose of this requirement is to ensure that the system can be installed and configured in a secure way before operational users have access to it. Therefore, the vendor defaults must be such that the correct level of security is achieved immediately whenever the product is installed.

In addition, the installation mechanism should provide facilities for setting and updating its configuration parameters, and for the initialisation of its protection-relevant data structures before any user or administrator policy attributes are defined.

For any particular security functionality component, there may be a range of possible parameter values varying from those offering negligible security to those offering stringent security. The diagram entitled Figure 4-1 on page 18 shows how the XBSS default value (highlighted) might lie in relation to vendors’ other values, contained within their systems.

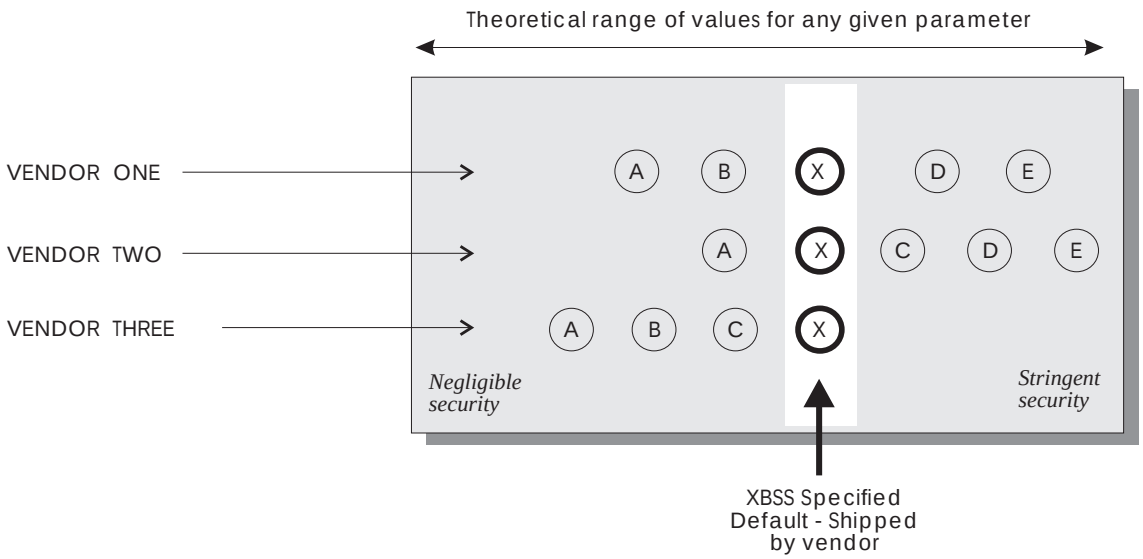


Figure 4-1 Examples of Possible Values

To achieve XBSS compliance, a vendor must supply the documented default, (X), but the vendor may also allow for a range of alternative values which exist to one side or to both sides of the default. Such alternative values are selectable only by an authorised user. This user may elect to select a different value at installation time, or sometime later when the system has been running and has been evaluated. In this way the key system parameters are established by someone who understands the security needs of the system. The setting of the parameters may be delegated to an authorised user who is installing the product. For any particular security parameter, if no alternative value is put in, then the value of that parameter will be the value documented in the XBSS.

For example, consider this normative requirement which is listed later in this chapter:

- **The TCB shall reject further login attempts if the authentication procedure is repeated unsuccessfully more than an administration-specified maximum on any given device or network connection.**
  DEFAULT: Five consecutive attempts at login only shall be permitted.

The shipped default is that rejection (of a user who is failing to login correctly) will commence after five login sessions have been attempted. This does not mean that this is the only way a system can run. The vendor is permitted to allow for other values, and for the end-user, site security policy may be such that a more strict value is selected. It is possible, for example, that a site might wish to invoke delaying mechanisms after the first failed login attempt.

4.3 Interpreting the Functionality Detail

The remainder of this chapter represents an itemised list of the individual requirements which represent the minimum specification for the XBSS. Each item is the technical requirement arising from the discussion of needs identified in Chapter 2. The default parameters which the suppliers must set to ensure that the system runs securely on delivery are plainly stated.

4.4 Identification and Authentication (I&A) Requirement

The requirements for identification and authentication consist of five primitives, addressed in Section 4.4.1 to Section 4.4.5 inclusive. This functional component is based on I&A-3 with additions. See Section B.2.2 on page 54.

4.4.1 Identification, Accountability and Audit

Requirement Detail

- **The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate.**
- **It shall not be possible to establish a session by any other means than by a documented interface.**
- **The TCB shall be able to perform individual accountability by providing the capability to identify each individual user.**
- **The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.**
- **By default user accounts shall be created with unique identities.**

Description and Rationale

The purpose of this requirement is to ensure that every user of the system is identified to it, that there are no provided mechanisms to by-pass this identification, and that consequently all actions of the user can be properly attributed to that user. In particular, user identification must be enforced for both login sessions established through connected devices, such as terminals or workstation keyboards, and through remote devices, such as network or dial-up connections.

Authenticated user identification provides the basis for additional security functions, for example access control and auditing.

All users of the system must first provide some form of identification so that the system has knowledge of who is using it. The identification dialogue procedure, or *login* must be successfully completed before any other communication with the system can begin. The login mechanism gathers the user's identification and propagates it to all subsequent actions taken by the user.

Newly created user accounts must not be associated with the resources or audit trail entries pertaining to past or present user accounts.

Note that this requirement does not prohibit an application from authorising anonymous access through dedicated terminals. In these circumstances the subject whose access is mediated by the TCB is the instance of the application. The user associated with the subject is the user that initially executes the application.

4.4.2 Authentication and Account Data

Requirement Detail

- **The TCB shall maintain authentication data that includes information for verifying the identity of individual users**
  DEFAULT: The primary method of authentication is by user password
- **as well as information for determining the product policy attributes of individual users (for example, groups, time intervals, location).**
- **This data shall be used by an uncircumventable TCB procedure to authenticate the user's identity and**
- **to ensure that subjects under the control of the TCB, created to act on behalf of the individual user, inherit the user's policy attributes.**
- **Upon execution a delayed session initiated on behalf of the user shall assume the attributes then current for that user.**
- **Delayed sessions shall not be executed on behalf of a user whose account has been disabled.**

Description and Rationale

For each user of the system, there must always be some form of data which authenticates that user. The usual form is the password and systems must be shipped equipped to deal with password authentication. However, it is perfectly reasonable to operate other authentication devices such as smart tokens, biometric measuring devices (such as a finger print or retina image), a challenge-response method, or a one time password list.

Having checked the authentication device, various other restrictions such as time of day, day of the week and location of use can be retrieved and enforced. (During the identification dialogue, data on time of login, port location or login machine can be collected for this purpose.)

All authentication and account data should be maintained in such a way that it can always be associated with the user during the *login* phase, and cannot be by-passed when the system verifies the identity of the user and initiates the user's session.

Various user parameters such as user ID, group ID, and supplemental groups are also retrieved and associated with all future user actions.

Various elements of account information are made available to all subjects operating on behalf of the identified and authenticated user. These include information for identifying the user in the audit trail and information for making *access control* decisions (such as the user's identity, group, and supplemental group membership).

For scheduled and delayed sessions, such as *cron* and *at*, further checks are made at the time of execution. In order for the delayed session to commence, the user's account must be enabled and the user's attributes must be correct.

For an explanation of *uncircumventable*, see Appendix E.

4.4.3 Authentication Data Protection

Requirement Detail

- **The TCB shall protect authentication data so that it cannot be used by any unauthorised user.**
- **The TCB shall appear to perform the entire user authentication procedure even if the user identification entered is invalid.**
- **The TCB shall reject further login attempts if the authentication procedure is repeated unsuccessfully more than an administration-specified maximum on any given device or network connection.**
  DEFAULT: Five consecutive attempts at login only shall be permitted.
- **Upon rejection a protected mechanism shall be invoked.**
- **This protected mechanism shall support both:**
  - **delaying subsequent login attempts on the affected device or network connection by an administrator-defined time**
    DEFAULT: The default action shall be to delay subsequent login attempts by 30 seconds.
  - **and disabling the user or account.**
- **Invocation of the protected mechanism shall be an auditable event.**
- **Invocation of the protected mechanism shall further invoke a mechanism which informs a security administrator or registers an alert.**

Description and Rationale

It is fundamental to security that the user's authentication data is not compromised by either disclosure or modification.

No authentication data, even if encrypted, should be available to unauthorised users. Clear text passwords should never be stored on the system, thus they will not be available to any user whatever the authorisation level of that user.

Disclosure would facilitate impersonation attacks. Modification could lead to denial of service. Furthermore, attacks on the user's authentication data are mitigated by not disclosing information about why a login failed, by discouraging repeated attacks through delaying or locking tactics, and by alerting appropriate site personnel.

The complete login cycle is to be performed even if an *invalid login* is noted before the login cycle is complete. This ensures that no useful information is given to an unauthorised user. Associated with the login procedure is a configurable maximum *login-failure* count. The *login procedure* is defined as being the time from when the first entry of identification information is made until the login is successful, or has exceeded the *login-failure* count, or a period of time elapses that is great enough to indicate no further login dialogue is taking place (a time out).

The delay of subsequent login attempts is a mechanism optionally to limit the frequency of such login attempts by means of an administrator-defined delay before login attempts can be restarted.

When the *login-failure* count is exceeded a protected mechanism is invoked that takes the appropriate action. This informing mechanism (also called an alerting mechanism) could be as simple as a shell script that sends mail, writes to the console or a defined terminal, or a call to the syslog mechanism that has been configured to alert a logged in user and record information in

the system log.

Optionally disabling the user or account must be provided as an alternative, but delaying with a configurable delay time is the default. The choice of whether to delay or lock an account depends on the site's policy. Locking accounts may be a safer action, but could also be used to deny legitimate service.

4.4.4 Active User Status Information

Requirement Detail

- **The vendor shall define the status information[3] associated with:**
  - **— all active users**
  - **— all user accounts (enabled or disabled).**
- **The TCB shall have the capability to maintain the status information.**
- **The TCB shall have the capability to protect the status information.**
- **The TCB shall have the capability to display the status information.**

Description and Rationale

This requirement is included in identification and authentication (I&A) because it is associated with getting an account started, and with system entry generally. Status information can show many things. It can include whether a user is logged on, what authorisations the user has, and so on. It is system specific. The requirement is that, where you have this information, and it is security sensitive, the facility to protect it must be in place.

This information is required to allow an administrative user to monitor and maintain the system.

The information shown at any given time may vary, according to the level of authorisation the user has within the system.

4.4.5 Specific Requirements for Password Authentication Mechanisms

In eight areas listed below there are requirements which provide a greater likelihood that passwords will not be compromised. They ensure that normally only the owner of the password can change it, that passwords are changed with regularity, that old passwords are not immediately reused, that passwords are sufficiently complex that they are not easily breakable, and that they are not visible to any other user.

3. As defined in the Conformance Statement.

Requirement Detail

Note: This requirement does not apply to systems where the system requires the use of a one-time password mechanism.

1. User-changeable Password

- **The TCB shall provide a mechanism to allow passwords to be user-changeable.**
- **Normal users shall only be authorised to change their own passwords.**
- **This mechanism shall require normal users to re-authenticate before changing their password.**
- **Administration shall have a mechanism to initialise or change passwords for users.**
- **By default new accounts shall have passwords set before the account is enabled for use.**
- **Administration shall have a mechanism to specify password expiration before first use.**
  DEFAULT: The new account created shall have the password expired.

2. Password Protection

- **It shall not be possible directly to derive the clear text password from the stored authentication data.**

3. Password Aging

- **The TCB shall be capable of password aging.**
- **A user's password shall be required to be changed after an administration-specified minimum time.**
  DEFAULT: The default time shall be 90 days.

4. Password Expiration

- **The TCB shall provide a mechanism to notify users in advance of requiring them to change their passwords. This shall be done by:**
  - **— notifying users during an administration-specifiable period of time prior to their password expiring.**
    DEFAULT: Each day for 7 days.
- **The TCB shall provide a mechanism to notify users when password change is due. This shall be done by one of the following:**
  - **— Upon password expiration, notifying the user but allowing a administration-specifiable subsequent number of additional usages prior to requiring a new password.**
    DEFAULT: 1 additional use.
  - **— Upon password expiration, the TCB shall notify the user at the time of login and require the password be changed before proceeding with the establishment of the login session.**

5. Password Reuse

- **The TCB shall provide at least one of the following mechanisms to prohibit password reuse:**
  - **— Passwords shall not be reusable by the same individual for an administration-specifiable period of time.**
    DEFAULT: The time period shall be 90 days.
  - **— Passwords shall not be reusable by the same individual for an administration-specifiable number of password changes.**
    DEFAULT: The number of changes shall be 10.
  - **— The user shall not be able to change the password again for an administration-specifiable period of time.**
    DEFAULT: The time period shall be 30 days.

6. Password Complexity

- **The TCB shall provide a method of ensuring the complexity of user-entered passwords that meets the following requirements:**
  - **— Administrators shall be able to configure at least the following two password complexity parameters: minimum length and "passwords shall not be all alpha" property.**
    DEFAULT: a six-character password which is not all alpha.
  - **— The password complexity-checking algorithm shall be configurable or replaceable by site.**

7. Password Logging

- **Plain text actual or attempted passwords shall not be displayed or logged.**

8. Default Passwords on Active Accounts

- **During installation or initial configuration, (for those systems that come pre-configured or have a configuration script), the TCB shall require default passwords to be changed.**

Description and Rationale

When an administrator sets up a user's account for the first time, the user must be given a password otherwise the user must not be able to log in. The administrator is to be able to mark the password as expired, thus forcing the new user to give himself a new password at his first login session. Using this method of password use, passwords are kept secret from administration. Company policy might view this as desirable (high security and accountability) or it might take the view that it is inconvenient and potentially costly (employee absent from work and his files are locked). Therefore it is important that the site can choose which password policy to adopt.

The administrator's guide should warn that the audit failed login record might show the user password instead of the user name in cases where users sometimes absent-mindedly enter their passwords before their userids and the system would then log the password as an invalid userid.

To ensure password protection, either the stored authentication data must be encrypted with a one way encryption method, or the authentication data must never be visible to any user. Ideally both should be true. It must not be possible for a user to obtain the clear text password,

even when that user has database or programming skills.

It is important that passwords are changed regularly to maintain security. Users are therefore forced to consider their password requirements every few weeks. If they are allowed to keep the same password for long periods of time, the risk of it becoming known would grow. Alternatively, if they are forced to change their password every few days they might not respect such a policy and might begin to write down their ever-changing password. The 90 day default age is considered to be a reasonable compromise between the extremes.

Some mechanism is to be present to let users know that their password is about to expire. This can be viewed as a machine implementation of good practice. Advance warning can be sent to the user by electronic mail, by notifying the user with a message at login time, or both.

Once a password has expired, a site must be able to configure how many times the old password can be used. A subsequent usage counter can be set to values 0, 1, 2, or *n*.

When 0 is set, the account is locked. The user is not offered the opportunity to change the password and must request intervention from the system administrator.

When set to 1, the user is told that the password has expired and that a new one must be chosen in order for the current login to be successful.

When set to *n*, the user is told that the password has expired. The user may elect to change the password immediately. If the password is not changed immediately, then *n*-1 login sessions will be allowed using the old password.

Note that if the value *n* is set to less than two, the user effectively has no prior notice of the requirement to change the password.

The password change mechanism must ensure that the new password offered is not the same as the expired password. Users tend to want to keep their passwords as long as possible, which, if allowed would lead to a deterioration of security strength.

The password complexity must at least be configurable to include a minimum length and whether a password consisting of all letters is acceptable, or whether some combination of letters, numbers, and special characters is required. For some usage models it is desirable for the password complexity checking to be highly configurable (for example, to include dictionary lookup), or replaceable by locally written code. This requirement allows for both, but requires at a minimum the default algorithm be configurable as to minimum length and alpha content.

When a system is delivered and before normal users are configured, login accounts may need to be used. These accounts should be protected by a default password, which is to be changed to a site password upon first login.

Some systems ship with accounts which have passwords but which are locked, uucp for example. There is no reason to change the password on an account which is locked and is therefore not subject to attack.

4.5 Basic System Entry Control

The basic system entry control functional component consists of five primitives, addressed in Section 4.5.1 to Section 4.5.5 inclusive. This functional component is based on SE-1 with additions. See Section B.2.3 on page 54.

4.5.1 Warning on Unauthorised Use

Requirement Detail

- **Prior to initiating the system login procedure, the TCB shall be capable of displaying a site-configurable advisory warning message to the user.**

Description and Rationale

The purpose of this requirement is to display a legally meaningful form of words (which might also include a welcome message or identifying message) to any potential user of the system before or during the login proceedings.

The message informs users that the system is security-aware. Such a message may contain legal warnings about use or misuse of the system. The strength of such a warning is a matter for company policy. For example:

```
XYZ System.  Warning:  You will be prosecuted to the fullest
extent of the law if you make an unauthorised
or illegal entry to this system
```

4.5.2 Authentication

Requirement Detail

- **Before system entry is granted to a user, the identity of that user shall be authenticated by an uncircumventable TCB procedure.**

Description and Rationale

The purpose of this requirement is to ensure that all users of the system are who they say they are.

Before the user is provided with a session on the system, the authentication mechanism must have verified the user's identity with the authentication data for that user. There must be no login mechanism that allows the authentication mechanism to be by-passed.

4.5.3 Information Displayed Upon Entry

Requirement Detail

- **Upon successful entry to the system, the TCB shall display the following data to the user and shall not remove it without user intervention:**
  - **— the date, time, origin, and service providing the last successful entry to the system and**
  - **— a representation of the number of unsuccessful attempts to access the system since the last successful entry by the identified user.**

Description and Rationale

The purpose of this requirement is to provide the user with information about the user's system entry activities. Here are examples of typical last login messages:

```
Last login: Thu Oct 13 09:41:11 BST via ftp from 192.1.2.3

4th unsuccessful access: attempted login on tty05 at Fri Oct 14 23:32:55
```

Should the user's account have been penetrated, these messages should be sufficient for the user to recognise that penetration, report it to the proper authorities, and take action to prevent future unauthorised use.

The representation of the number of successive, unsuccessful events could be that of a count (integer value), a list of the timestamped unsuccessful attempts, or some other such representation.

This encourages users to be responsible for their own security, for it is they, more than anyone else, who are likely to spot an anomaly such as a login at a strange time of night at an unusual terminal.

4.5.4 Pseudo-users

Requirement Detail

- **The TCB shall be capable of restricting pseudo-users from establishing a login session when the system operates in normal mode.**
  DEFAULT: This feature is activated.

Description and Rationale

The purpose of this requirement is to ensure all the human users identify themselves to the system with an identity which is uniquely associated with them, for accountability purposes.

When the feature is activated, a direct login for an account with unrestricted privileges, such as the login as *root* is not allowed.

When authorised, users can gain the authorisations associated with pseudo-user identities through appropriate mechanisms within their login session, such as **su**. See also Section 4.8.6 on page 41.

4.5.5 User-initiated Locking

Requirement Detail

- **The TCB shall provide a mechanism for user-initiated locking of the user's own interactive sessions that includes:**
  - **— requiring user re-authentication prior to unlocking the session**
  - **— disabling any activity of the user's data entry other than unlocking the session.**

Description and Rationale

The purpose of this requirement is to provide a mechanism, short of logging out, by which a user can leave a terminal (or monitor) and be assured that no other person can make use of the user's session.

During the time that the user session is locked it may be desirable, though it is not required, to disable output and clear or occlude the screen.

4.6 Basic Audit Requirement

The basic audit functional component consists of four primitives, addressed in Section 4.6.1 to Section 4.6.4 inclusive. This functional component is based on AD-2 with revision. See Section B.2.5 on page 55.

4.6.1 Authorised Control and Protection of the Audit Trail

Requirement Detail

- **The TCB shall be able to create an audit trail of accesses to the objects it protects.**
- **The TCB shall be able to maintain an audit trail of accesses to the objects it protects.**
- **The TCB shall be able to protect from:**

  — modification

  — unauthorised access or

  — unauthorised destruction

  an audit trail of accesses to the objects it protects.
- **The audit data shall be protected by the TCB so that read access to it is limited to those who are authorised for audit data.**

Description and Rationale

The purpose of this requirement is to ensure that the audit trail data is protected from unauthorised reading, writing, or destruction.

If the audit trail was available for normal users to read, they could determine what activities were being audited and change their actions based on that knowledge. This would negate the deterrent effect of auditing. If the audit trail was available for writing by normal users, they could enter records that were misleading, or could flood the audit trail and deny access to it. If the audit trail was available for destruction by normal users, they could erase evidence of their wrong-doings.

However, the audit trail needs to be protected at a level beyond that of the malicious or irresponsible action of normal users. If an intruder can defeat a system's access control mechanisms, and assumes all the rights and powers of a administrative user, it would be extremely useful to be able to audit the intruder's activities. The intruder, as a administrative user, would seek to modify the audit trail to remove the evidence of the break-in. Therefore, the audit trail should not be alterable even by a administrative user and the only real safeguard to prevent audit files being overwritten or destroyed is to write the audit messages to a write-only medium or to a physically secure host somewhere else on the network. In truth, it is difficult to protect against the system-skilled intruder.

In reality, a certain level of protection can be provided by ensuring that the interfaces to create, destroy, read, and write the audit trail are protected so that they can only be used by system subjects. For example, the system calls can only be placed by the privileged application. The audit trail file and containing directory have *access controls* that only allow read, write, and search access to the privileged application and read and search access to members of a group to which only authorised users belong.

There is a secondary implication that the system is to have the ability to audit access to its protected objects. That is the objects for which it mediates *access control* as specified in these requirements.

4.6.2 Recordable Security-relevant Events

Requirement Detail

- **The following types of events shall be capable of being recorded, when enabled and when recording space requirements are met:**
  - **— use of the identification and authentication (I&A) mechanism, system entry and exit, and session initialisation and termination events shall be recorded by default**
    DEFAULT: Upon system delivery the recording of these events shall be enabled.
  - **— access control events selectable on a per user, per group, per subject, per object basis; security-relevant access control events are:**
    - **— association of objects with subjects**
    - **— creation and deletion of subjects and objects**
    - **— distribution and revocation of access rights**
    - **— acquisition and deletion of system privileges**
  - **— actions taken by administrative users including:**
    - **— modification of TCB elements**
    - **— audit trail control and management**
    - **— accesses to TCB objects**
    - **— changes of policy attributes of users**
    - **— changes of TCB configuration**
    - **— selection and modification of audited events**
  - **— and all other security-relevant events.**
- **The events that are required to ensure integrity of the audit trail shall be identified in the Administration Documentation and:**
  - **— shall not, by default, be disabled[4]**
  - **— interdependencies of audit events shall also be identified in the Administration Documentation and**
  - **— attempts to disable logging of events upon which another enabled event depends, shall generate a warning or be prevented.**
- **The TCB shall provide a protected mechanism that displays the currently selected events.**
- **The use of this mechanism shall be restricted to authorised users.**

4. This should not be interpreted to mean that an authorised user cannot turn auditing off. See section 4.6.4 Audit Trail Control.

Description and Rationale

The purpose of this requirement is to specify the minimum types of audit events that are recordable and to specify which events must *always* be recorded when auditing is activated. It is permissible, and it may be desirable, for vendors to specify types of audit event in addition to the minimum.

However, auditing has implications for system efficiency. Heavy use of auditing will bring about system degradation, with large amounts of time being allocated to the generation of audit records and to the interpretation of audit records. The audit data will also take up a significant amount of storage space. Therefore, the recording of events is conditional on auditing being enabled, the recording of the particular event being enabled, (preselection), and upon audit trail space being available to record the event.

As a minimum audit requirement, the following activities should be recordable:

- successful and failed attempts to establish a login session
- use of the *open*, *creat*, *unlink*, *fork*, *exec*, *exit*, *chmod*, *chown*, *setuid* and other system interfaces
- administrative changes to system databases, including changes to user account attributes, audit trail configuration and analysis, assigning set-user-id to programs, adding or changing system programs or procedures, changing the date or time.

Events that are required for the audit trail to be comprehensible must always be recorded.

Consider this example:

> A user changes his identity through a command such as *su*. If the method of ensuring that the accountable user for future actions is to trace back changes in identity and process ID to the initial system entry audit record, then all process creation and all user identity changes must always be recorded in the audit trail, and it is essential that those events would never be disabled.

All methods for viewing the audit events which are currently selected are restricted to an administrator and there can be no alternate method or workround for users to view which events are selected or to tamper with the selection.

4.6.3 Data Recorded for Each Event

Requirement Detail

- **For each recorded event, the following information shall be available:**
  - **— date and time of the event**
  - **— user**
  - **— type of event**
  - **— success or failure of the event.**
- **For identification and authentication (I&A) events, the origin of the request (for example terminal ID) shall be included.**
- **For events that associate an object with a subject and for object create and delete events, the audit record shall include the name and policy attributes of the object.**

Description and Rationale

The purpose of this requirement is to specify the minimum information that must be recorded in audit records. Each audit record must record *who* initiated the event, *what* happened, *when* it happened, *to whom* it happened (where applicable), and *how* (or why) it happened.

Though not explicitly required for all audit records, *where* it happened is also required, perhaps only by the ability to trace the audit record back to the initial system entry event for the session in which this event took place.

It is permissible to record more information, and this may be desirable in certain cases.

For Identification and Authentication (I&A) system entry events, *where* the user entered the system is required. This information could take the form of the machine's name (network address, or some string) and the physical device (such as **tty1**, or **console**) for local and hard-wired connections, or the local and remote machine names (network address) and a port of entry (and peer port) identification, for networked connections.

If an object (the *to whom*) is associated with the action being reported, that object's name (or the ability to find the object's name) and its policy attributes are to be included in the audit record. In cases where a policy attribute included an Access Control List (ACL), it would be prudent to have an option to exclude the ACL from the audit record simply because its potential size is so great. It is possible to use an inode number for an file object name if the audit trail contains a mapping from that inode number to the file name and all creation of new name/inode number mappings is always recorded. The policy attributes are required for the selection of audit records described in Section 4.6.4 below.

4.6.4 Audit Trail Control, Management and Inspection

Requirement Detail

- **The TCB shall provide a protected mechanism for turning auditing on and off, and**
- **to select and change the events to be audited and their defaults during system operation.**
- **The use of this mechanism shall be restricted to authorised system administrators.**
- **The system administrator shall be able selectively to audit the actions of one or more users based on identity or object policy attributes.**
- **Audit review tools shall be available to authorised personnel to inspect and review audit data.**
- **These tools shall be protected from unauthorised use.**
- **These tools shall be protected from unauthorised modification.**
- **These tools shall be protected from unauthorised destruction.**
- **The TCB shall provide protected audit trail management functions that shall enable:**
  - **— creation, destruction and emptying or archiving of audit trails**
  - **— notification of the system administrator of the imminence of audit trail capacity thresholds being exceeded and**
  - **— the ability to take the least disruptive or administrator specified action to resolve the situation when free space is exhausted. The actions shall include at least the following:**
    (a) Raise a periodic alarm and discard unrecorded audit material
    (b) Suspend activities which result in the generation of auditable events

DEFAULT: (a) Raise a periodic alarm and discard unrecorded audit material.

— **formatting and displaying of audit trail data**

— **maintaining the consistency and continuity of audit trail data as part of system recovery after failure.**

Description and Rationale

The purpose of this requirement is to specify how the audit trail is to be configured and managed, as well as reviewed. Reviewing the audit trail takes the form of analysing the data stored there, tracking interesting sessions, generating reports, and so on. All methods for manipulating the audit state and reviewing audit data are to be restricted to authorised personnel and protected from tampering or use by normal users. If normal users could manipulate the audit state, they could defeat its effectiveness. If they could review audit data, it could provide them information for which they are not authorised as well as defeat the deterrent effect of audit.

To secure the audit functionality, the audit tools could be stored in directories which are only readable, searchable and executable by an audit group to which only authorised administrators are members. The audit data files are assigned read only access to the audit group.

This requirement calls for both preselection (configuring which events are to be recorded in the audit trail) and post-selection (the selection of audit records from the recorded audit trail). Preselection is desirable because it reduces the amount of audit data that is stored, but it must be kept in mind that if an event is not preselected to be recorded in the audit trail, it cannot be post-selected for when the audit trail is analysed.

By default, the post-selection tools must be able to select audit records based on the identity of users and the policy attributes of objects they access.

When the storage space for the audit trail is nearly full the system has to notify appropriate personnel. The documentation on the security aspects of the installation must suggest a course of action which the appropriate authorised user would take to resolve the situation in the least disruptive way.

If the audit trail becomes unavailable (either full or off line) then various courses of action are possible:

- processes that causes audited events to be generated can be put on *sleep*
- the system can be halted
- unrecorded audit records can be discarded — counter could record how many audit records have been discarded.

However, the discard method must not be *the only* method of dealing with an unavailable audit trail.

4.7 Basic Access Control Requirement

The basic access control functional component consists of four primitives, addressed in Section 4.7.1 to Section 4.7.4 inclusive. This functional component is based on AC-1 with additions and revisions. See Section B.2.6 on page 55.

4.7.1 Access Control Attributes

Requirement Detail

- **The TCB shall define access control attributes for subjects and objects.**
- **The TCB shall protect access control attributes for subjects and objects.**
- **Subject attributes shall include a named user or a named group or both.**
- **Object attributes shall include the defined access rights of read, write and execute that can be assigned to subject attributes.**

Description and Rationale

The purpose of this requirement is to specify the access control attributes of subjects and objects and to assure that they are protected. The access control attributes of subjects are at least: named users, the effective and real user ID of the subject, named groups, the effective and real group ID of the subject and the supplemental groups of the subject. The access control attributes of objects are at least: read, can read data and view attributes, write, can write data and modify attributes, execute, can execute the contained program, or search a directory.

These must be individually assignable to named users and named groups. In an XPG4 system, processes have user and group ID, files have read, write, and execute permissions to the owning user, owning group, and others, directories have read, write, and search permissions to owning user, owning group, and others. Access control to processes is limited to identical user IDs.

4.7.2 Rules for Access Control Attributes

Requirement Detail

- **The TCB shall define rules for assignment and modification of access control attributes for subjects and objects.**
- **The TCB shall enforce rules for assignment and modification of access control attributes for subjects and objects.**
- **The effect of these rules shall be that access permission to an object by users not already possessing access permission is assigned only by authorised users.**
- **These rules shall:**
  - **— allow authorised users to specify and control sharing of objects at minimum by owner and one named group, and**
  - **— shall provide controls to limit propagation of access rights.**
- **The rules for assignment of access control attributes shall include those for attribute assignment to objects during import operations.**
- **The rules for modification of access control attributes shall include those for attribute assignment to objects during import operations.**

- **The rules for assignment of access control attributes shall include those for attribute assignment to objects during export operations.**
- **The rules for modification of access control attributes shall include those for attribute assignment to objects during export operations.**
- **If different rules for assignment and modification of access control attributes apply to different subjects or objects, the totality of these rules shall be shown to support the policy defined by the TCB.**

Description and Rationale

The purpose of this requirement is to specify who should grant access to objects and to whom access may be granted. Only an authorised user can grant access to an object. Having access to an object does not grant the right to give any other user access to that object. If a subject currently has access to an object and an authorised user revokes that access, the revocation need not be immediate, but may take place when the next access is requested. In an XPG4 system the only authorised user is the object's owning user. The owning user can modify the owning users access rights and at least one named groups access rights. Modifying the other access rights is also permitted. If the system allows for finer grained access control such as Access Control Lists (ACLs), this requirement limits the granting of access to the owner (or delegate, if supported and specified by the owner) for any named users or named groups in the ACL.

4.7.3 Authorisation of Subject Access to Objects

Requirement Detail

- **The TCB shall define authorisation rules for the uncircumventable mediation of subject access to objects.**
- **The TCB shall enforce authorisation rules for the uncircumventable mediation of subject access to objects.**
- **The rules shall be based on the access control attributes of subjects and objects.**
- **These rules shall, either by explicit user action or by default, provide that objects are protected from unauthorised access.**
- **The scope of the authorisation rules shall include a defined subset of the product's subjects and objects and associated access control attributes.**
- **The coverage of authorisation rules shall specify the types of objects and subjects to which these rules apply.**
- **If different rules apply to different subjects and objects, the totality of these rules shall be shown to support the policy defined by the TCB.**

Description and Rationale

The purpose of this requirement is to ensure that all access to controlled objects is mediated such that access is only granted based on the requirements in Section 4.7.2 on page 35, to ensure that when an object is created default access attributes are associated with it, and to require that the system define which objects are controlled. For example, in an XPG4 system, the access rules for a file should be that the owning user of the subject must be granted the requested access by the permission bits (or ACL) of the file. When a file is created, it is given the owning user and owning group of the process that created it and the permissions as specified by the creating process' umask.

The system is to define all types of subjects and objects it controls and specify the access rules it enforces for all the controlled types of subjects and objects.

4.7.4 Subject and Object Creation and Destruction

Requirement Detail

- **The TCB shall control the creation and destruction of subjects and objects.**
- **These controls shall include object reuse.**
- **That is, all authorisations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects.**
- **Information, including encrypted representations of information, produced by a prior subject's actions, shall be unavailable to any subject that obtains access to an object that has been released back to the system.**

Description and Rationale

The purpose of this requirement is to ensure that subjects and objects cannot be created in a way that would compromise the information protected by the system. In order to ensure this the creation and destruction of all subjects and objects must only be done by the system. Subjects may request that the system create and destroy subjects and objects, but they have no ability to do so themselves.

Whenever a subject or object is created, the system has to ensure that the *resources* used to create the subject or object do not contain any information from a previous use. Examples of these resources are:

- Processes — the registers, text, data and stack memory when running a new program and any additions made to memory by the running program.
- Regular files — the files, attributes and disk storage allocated for data and attributes.
- Directories — the disk storage allocated for directory entries.
- Symbolic links — the disk storage allocated to hold the link contents.
- Special files — the attributes and media data.
- Pseudo-terminals — the attributes and data buffers.
- FIFOs — the attributes and data buffers.
- Pipes — the attributes and data buffers.
- Message queues — the initial content and data buffers.
- Semaphores — the initial content.
- Shared memory — the initial content.

4.8 Basic Security Control

The basic security management functional component consists of six primitives, addressed in Section 4.8.1 to Section 4.8.6 inclusive. This functional component is based on SM-2 with additions. See Section B.2.8 on page 55 and on PO-1, with specific roles defined, see Section B.2.14 on page 56.

4.8.1 Secure System Setup and Initialisation

Requirement Detail

- **The TCB shall provide an installation mechanism for the setting and updating of its configuration parameters, and**
- **for the initialisation of its protection-relevant data structures before any user or administrator policy attributes are defined.**
- **It shall allow the configuration of TCB internal databases and tables.**
- **The TCB shall distinguish between normal mode of operation and maintenance mode.**
- **At least the following operations shall be performed in maintenance mode:**
  - **— recovery of the TCB, and**
  - **— system start-up to resumption of full system operation.**
- **Mechanisms shall prevent a normal user from placing the system into maintenance mode.**
- **Mechanisms shall prevent a normal user from interacting with the system while in maintenance mode.**

Description and Rationale

The purpose of this requirement is to ensure that the system can be installed and configured in a secure way before normal users have access to it. It is also to distinguish modes of operation.

Maintenance mode is intended to be a mode for administrative users to perform operations which cannot securely be done when other users are present. For example, if the TCB has been corrupted such that safe operation cannot be assured, the system should be operated in maintenance mode with access restricted only to authorised administrators to correct the corruption. Mechanisms have to protect entry into maintenance mode by normal users.

Note that not all system maintenance is intended to be performed in maintenance mode, particularly backups or regular system maintenance which does not affect the TCB. Repair operations on damaged resources which are not part of the TCB and to which access is restricted to administrative users also need not be performed in maintenance mode.

An example of the types of configurations required before normal user access is the configuring of initial user and administrator accounts, home directories, audit parameters, configuring the system audit trail, and the setting of appropriate access controls on files and directories in the system.

4.8.2 Security Policy Parameters

Requirement Detail

- **The TCB shall provide protected mechanisms for displaying and**
- **modifying the security policy parameters.**
- **These parameters shall include identification, authentication, system entry and access control parameters for the entire system and for individual users.**
- **The system shall be supplied with secure defaults where appropriate such as for policy attributes for subjects and objects.**
  DEFAULT: The default supplied shall be to limit access to the creator of the object only.
- **User-settable defaults shall also be secure.**
- **The TCB shall have the capability to define the identification and authentication policy on a system wide basis.**
- **The system shall be provided with a secure default for locating executable programs.**
  DEFAULT: The default user's environment shall not search directories writable by any normal user nor automatically search the current directory when locating an executable program.

Description and Rationale

The purpose of this requirement is to ensure that the mechanisms for accessing and modifying the security policy parameters of the system are protected from tampering and therefore can be trusted for correct operation, and to specify the identification and authentication policy and associated parameters. Additionally secure policy defaults have to be applied. For example: Update access to TCB files must be limited to authorised personnel. Access to user's data must by default be to the owning user. The user's default *umask* must be `077`.

The number of unsuccessful login attempts must be specifiable by authorised personnel through a trustworthy interface.

The default setting for locating executable programs will typically be implemented by using the search path defined in the PATH variable. The intent is that, by default, executable programs will only be searched for in defined controlled system directories; this may overridden by individual users as desired. The system default search path should, however, not include the user's own directories.

4.8.3 User Registration Data

Requirement Detail

- **The TCB shall provide protected mechanisms for manually displaying user registration and account parameters.**
- **The TCB shall provide protected mechanisms for manually modifying user registration and account parameters.**
- **The TCB shall provide protected mechanisms for manually deleting user registration and account parameters.**
- **The TCB shall provide protected mechanisms for manually disabling user registration and account parameters.**

  - **For the preceding four requirements, the parameters shall include unique user identifiers and their account.**

- **The TCB shall allow the automatic disabling of user identities or accounts after a period during which the identity or the account have not been used.**
- **The time period shall be administrator specified, with a specified secure default provided. *DEFAULT: 30 days*.**
- **The administrator shall have the ability to re-enable disabled user identities or accounts.**
- **The TCB shall provide a means to identify security policy attributes.**
- **It shall also provide a means for authorised users to list these attributes.**
- **It shall be capable of defining and maintaining the security policy attributes for users.**

Description and Rationale

The purpose of this requirement is to define the required mechanisms for accessing and modifying user account parameters, and to ensure that the mechanisms are protected from tampering and therefore can be trusted for correct operation. In defining these mechanisms the minimum account parameters are also specified.

Examples of TCB security policy attributes that should be defined and maintained include: privileges for privileged users, such as security administrators; membership of users in groups; and user roles and capabilities.

A facility for re-enabling of disabled accounts provides a counter to the denial of service that could come if an account were automatically disabled for excessive failed login attempts.

4.8.4 System Resources

Requirement Detail

- **The TCB shall provide protected mechanisms for ensuring that only authorised personnel are allowed to perform tasks associated with control and maintenance of system resources.**
- **It shall allow:**
  - **the enabling and disabling of peripheral devices**
  - **mounting of removable storage media**
  - **backing up and recovering user objects**
  - **maintaining and testing software elements**
  - **starting and shutting down the system.**

Description and Rationale

The purpose of this requirement is to ensure that the mechanisms for controlling the system are protected from tampering and therefore can be trusted for correct operation, that only appropriate personnel have the ability to restore objects to the system that they do not own, that only appropriate personnel have the ability to shut down and reboot the system, and that only appropriate personnel have the ability to control access to removable media devices.

The definition of appropriate personnel is specific to a site. What is required of the system is that there is a capability that can be employed to limit these actions to whomever the site believes is appropriate.

An example of control over removable media is, diskette, tape, CDROM, etc. interfaces to the system have access controls that are settable by appropriate personnel.

4.8.5 Restriction on Use of Administration Functions

Requirement Detail

- **Security sensitive administrative functions shall only be successfully performed by appropriately authorised users.**

Description and Rationale

The purpose of this requirement is to ensure that normal users cannot change the security parameters of the system. The successful use of all the functions that modify system wide or user specific security parameters must be protected. These can be protected by appropriate access control on data bases such that modification is restricted to appropriate personnel. Further restrictions on use of TCB interfaces can be limited to the appropriate administrative user.

4.8.6 Administration Functions

Requirement Detail

- **Administrative functions shall be provided such that normal system administration can be accomplished without granting additional access rights to objects other than those necessary to perform the specified administrative functions.**
- **These functions shall be configurable so that administrators can be assigned access to arbitrary sub-sets of the functions listed below.**
- **Mechanisms shall be provided for associating authorised users with administrative functions.**
- **The minimum set of system administration functions shall include:**
  - **— adding and removing users (including granting authorisations, and password management of users)**
  - **— password management of users**
  - **— modifications of access controls**
  - **— control of audit (including review of audit)**
  - **— review of audit only**
  - **— backup and restore**
  - **— backup only**
  - **— configuring system defaults and parameters**
  - **— system shutdown.**

Description and Rationale

The intent of this requirement is to allow customers to configure the system to support disjoint administrative roles to meet the business requirements and the site security policy regarding administration. Each role can be defined by the customer as a combination of the administration functions.

It should not be necessary to use the super-user capability in day-to-day administrative tasks. As a consequence, the number of human users with access rights to the super-user capability can be limited.

This requirement explicitly lists a minimum set of administrative functions associated with security objects. XBSS compliant systems are expected to provide a similar level of granularity for other administrative functions, such as print/spool, networking, mass storage, terminals, or software package administration. Such a list cannot be included in the requirement as it is system-dependent.

No default settings are associated with this requirement. Note that the requirement on pseudo-user login abilities (see Section 4.5.4 on page 28) implies the creation of administrative users and their association with the system administration functions is required before the system can be brought in the normal mode of operation for the first time.

Note that the term ‘‘normal system administration’’ is explained in **normal system administration** on page 73.

4.9 Trusted Recovery

The trusted recovery functional component is composed of a single primitive, addressed in Section 4.9.1. This functional component is based on TR-1 with revisions. See Section B.2.13 on page 56.

4.9.1 Trusted Recovery After Failure

Requirement Detail

- **Procedures shall be documented to ensure that, after a TCB failure or discontinuity, recovery which minimises protection compromise is obtained. Reinstallation may be required to achieve this and in most cases may be the only, the most practical and the prudent thing to do to ensure all security services are fully in effect.**
- **Trusted recovery shall take place in maintenance mode.**

Description and Rationale

The purpose of this requirement is to ensure the integrity of the TCB following a system crash or unauthorised user shut down. Re-installation may be the safest and easiest course of action, some checking may be performed, if the tools are provided and the expertise is available, that enable continuation of service without re-installation. The expertise alluded to would be that required to make an assessment of the level of protection compromise.

The XPG4 file system check program is a necessary, though not sufficient, part of an automated procedure to meet this requirement. Either an administrative procedure or automatic mechanism that assures all the TCB components (programs, libraries, data bases) are in a known defined secure state and have suffered no compromise is required. A potentially acceptable mechanism would be to verify the ownership, access rights, and contents (potentially through a cryptographic checksum) of each component of the TCB.

Another potentially acceptable method for the static components of the TCB would be to have them reside on immutable media such as on an immutable file system or a CDROM.

4.10 Security Manuals

The Security Manuals functional component is comprised of two primitives defined in Section 4.10.1 to Section 4.10.2 inclusive. This functional component was added by the X/Open Security Working Group. See Section B.3 on page 57.

4.10.1 User Documentation

Requirement Detail

- **The vendor shall provide end user documentation in the form of a single summary, chapter, or manual which:**
  - **— describes the security facilities that the end user is likely to have to use, why they are important and any special considerations or guidelines for their use**
  - **— describes symptoms of security problems that the end user is likely to encounter and should be on the look- out for, why they are serious and what actions he should take**
  - **— points to the reference guide, where all end user security facilities are fully defined.**

Description and Rationale

The purpose of this requirement is to ensure that the users of the system have all the information they need to operate it in a secure manner from day one. The information relating to security should, by preference, be contained in one particular manual, but it is acceptable for it to be contained in a number of manuals in the standard user documentation set, provided the user can readily determine where to find all the relevant security features. The information on security can either be delivered with the system, or a clear pointer to its availability should be included.

The ultimate aim of the security documentation for the user is to foster good working practices. It is more difficult for a user to blame ignorance for a breach in security if there is no excuse for such ignorance. Security need never slide towards the lowest level of enforcement. With users performing their tasks at an optimum level of security, the overall efficiency of both human and computer can be raised, and demands upon the time of the system specialist can be reduced.

4.10.2 Administration Documentation

Requirement Detail

- **The vendor shall provide product administrator documentation which describes the proper administration of all the security services and associated procedures, privileges, and functions.**
- **This documentation shall describe the administrative interaction between security services, and shall provide guidelines on secure generation of a new TCB.**
- **The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.**
- **The vendor shall provide a set of criteria that an application has to meet in order to guarantee that it can be added to the TOC without compromising conformance to this specification.**

Description and Rationale

The purpose of this requirement is to ensure that the product administrator has the materials to understand how to administer the system in a secure manner. The manual may give general security advice (an overview), but specifically it should:

- explain clearly how to install (or re-install) and then configure the system in a secure manner — this would involve some discussion of the user and the user account, group membership, subject attributes and object attributes
- explain how to maintain the system in a secure manner across its life time — this might include examples of daily, weekly and monthly security routines as well as specific tasks such as bringing a system backup after a crash
- provide instruction on how to regenerate parts of the TCB, such as the kernel, in a secure way (on systems that allow TCB regeneration)
- explain the audit trail mechanism so that the authorised user can effectively use the audit trail to implement the local security policy
- explain how to adjust system defaults if experience of use shows them to be too lenient or too stringent.

The documentation should not be written in a language or tone that requires the reader to be a system expert. System security is often perceived as an costly option, achieved only by procuring special expertise. Yet the business world sees security administration as a routine job, the post for which is usually filled from the administrative/clerical labour pool, not necessarily from the technical/programming labour pool where shortages abound.

Clear documentation giving specific instructions for specific security-related tasks (such as system backup) could simplify security administration and reduce overall system costs.

The requirement for criteria for adding to the TOC in a secure manner is expected typically to be met by enumerating the ways in which a program executing on the system can be given, or acquire, privileges which may be exploited in order to circumvent the system security policy. This is likely to include, but not be limited to, execution by users with special authorisations (in particular the root user), assignment of set-user-id permissions to executables, and execution by privileged system processes (for example the login process, or a network services daemon).

Since the primary audience for the stated document is system administrators who will be installing third party applications programs, it will be helpful to give guidance both on how to install an application with secure default permissions and on how to detect potential use or abuse of privilege subsequent to the installation. This may be as simple as instructions on checking for the presence of set-user-id executables on the system, or be extended to include advice on analysis of the system audit logs.

Appendix A

X/Open Branding

X/Open branding is the procedure by which a vendor warrants that its product complies with one or more of X/Open Company's vendor-neutral open systems specifications.

It is called branding because it is built around the right to use the X/Open trade mark, with trade mark law as its legal basis. Once the vendor warrants and represents that his product complies with the specifications, the vendor is entitled to use the X/Open trade mark, in the form of the branding logo, in relation to that product and its X/Open branded features. That right continues for as long as the product remains registered in the Register of X/Open Branded Products.

A.1 Background

In 1988, X/Open introduced a brand to act as a ready identifier for products that conform to the specifications published in the X/Open Portability Guide, Issue 2 (XPG2). In June 1990, X/Open launched the uniquely successful X/Open Portability Guide, Issue 3 (XPG3) branding programme. This was followed by XPG4 in 1992, which vastly increased X/Open Company's coverage of brandable technology. In general, XPGn is the name given to the set of brandable items in the X/Open Common Applications Environment (CAE) at a moment in time, and is supported by a branding programme that is based on the use of the specifications in the CAE. The X/Open CAE is a collection of both specifications developed by X/Open and its partners, and references to formal standards.

Use of the X/Open brand is strictly controlled by a comprehensive licensing agreement which sets out clearly the criteria for compliance for all types of X/Open-conformant products and establishes stringent rules and obligations in the use of the trade mark.

A.2 The X/Open Mission

One of X/Open Company's main tasks is to define common open systems specifications by helping major industry participants reach consensus. The results of this consensus-building process are to be seen in the publication of X/Open CAE specifications. However, this is only one element in X/Open Company's effort to pursue its mission statement.

This mission statement reads as follows:

To bring greater value to users from computing through the practical implementation of open systems.

To bring practical value to users, X/Open must by necessity do more than merely produce paper specifications. It must ensure that those specifications result in conformant products appearing in the market place. X/Open achieves this through the creation of the X/Open brand and supporting branding process.

A.3 Why the Brand is Important

The X/Open brand brings significant business benefits beyond basic certification programmes. These certification programmes simply indicate that a product could pass a test at that moment in time. The certificate makes no statement about implementation on a user site or system. The X/Open Brand on a product means that the vendor guarantees that the product complies to the specification, that it will continue to comply and that any non-compliances that may be subsequently found will be fixed within an agreed time.

The process of branding of X/Open-conformant systems is shown, in simplified form, in Figure A-1. below.

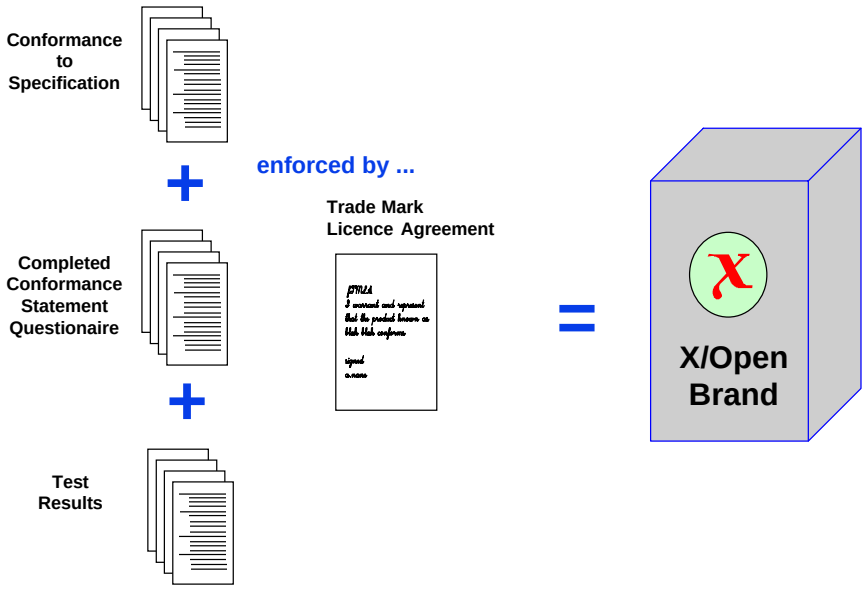


Figure A-1 Branding Process

The X/Open branding process makes use of several important elements:

- CAE technical specifications
- Component Definitions
- Profile Definitions
- Conformance Statement Questionnaires
- Verification test suites
- Trade Mark Licence Agreement.

Each of these has a vital role to play in ensuring that products that warrant conformance to X/Open specifications actually do conform in practice and continue to do so all the time they retain the brand.

A.4 CAE Specifications

These provide a highly detailed definition of what is required of a product in order to conform. Specifications are provided that cover a wide range of technologies and this coverage is increasing year by year. CAE Specifications are normally developed by X/Open technical working groups, but can also result from X/Open Company's *fast-track* process, in which the specification originates from outside X/Open. In these cases, the sponsoring organisation, acts as the editor of the specification as it passes through X/Open Company's formal adoption processes in order to be integrated into the X/Open CAE. X/Open places various requirements on specifications that enter the fast-track process. These are intended to ensure that the new specification integrates cleanly with the rest of the CAE.

A.5 Component Definitions

A Component Definition is the smallest functional element to which specific products may be separately branded under the X/Open branding programme.

A Component Definition corresponds to a coherent set of system or product capability, that is potentially broader than that contained within a single specification, and which can be implemented in a genuinely open manner by adherence to specific X/Open specifications. The particular specifications to be used are identified in the Component Definition. They may be X/Open specifications, other industry standards, or formal (de jure) standards.

Component Definitions are the building blocks of the X/Open integrated open system definition. Over time, X/Open is committed to providing more and more Component Definitions, and to increasing the scope of the Component Definitions already defined, in order to broaden the functional capability that is available in the open systems domain.

A.6 Conformance Statement

This is the third key element in X/Open branding and directly supports the CAE specification and Component Definition. As with all X/Open documents, the Conformance Statement, (CS), is a public document and effectively makes contractual obligations of the vendors for the procurers' benefit.

A Conformance Statement is defined to accompany each and every Component Definition and is intended to describe how a product conforms to the Component Definition and CAE specifications. For example:

- A specification may state that a conformant implementation may optionally support some particular feature. The Conformance Statement establishes beyond doubt, whether the product in question actually does support that feature.
- The specification may also specify a number of options from which the implementor may choose. In that case the Conformance Statement establishes which options are implemented by the product.
- The specification may state that a particular parameter or limit value is implementation-defined. In that case the Conformance Statement establishes the exact value for the implementation.
- The supplier is required to state in the Conformance Statement the precise equipment configuration that has been used to determine the conformance of the product to the X/Open Component Definition.

- Where the X/Open brand applies to a product in a range of binary compatible environments, the Conformance Statement allows the binary compatible family to be specified.

In addition, in the cases where it is impossible or economically not feasible to provide automated test suites, the Conformance Statement can aid in establishing exactly how conformance to the specification is demonstrated.

A supplier of a branded product is required to make a complete Conformance Statement Questionnaire available to prospective customers for examination prior to sale. Buyers of branded products are strongly recommended to obtain access to the X/Open Conformance Statement Questionnaire as it contains valuable information regarding the product and the way in which it conforms to the X/Open definitions.

A.7 Verification Test Suites

Test suites exist for many X/Open Component Definitions, and in such cases, the successful completion of a formal test is a prerequisite for X/Open branding.

Where X/Open does not specify a test suite for a component, no indicator of compliance needs to be presented at the time of branding. However, the supplier is still required to warrant and represent that the product conforms to the applicable X/Open definitions and none of his obligations under the Trade Mark Licence Agreement are in any way reduced.

For a number of X/Open Component Definitions, X/Open has itself developed conformance test suites which it has made available under licence through a network of distributors. In other cases, for instance in the programming language components where the X/Open specifications conform to international standards, X/Open references the test suites that have been developed to support the existing formal certification programmes for these languages in the U.S.A. and Europe.

The requirements in the Trade Mark Licence Agreement regarding continuing conformance of a branded product state that a supplier is required to ensure that any changes to a product have no effect upon its conformance. The implication of this is that the X/Open specified conformance test tools become embedded within the normal quality assurance process of the supplier. Through this means the supplier is able to retain the brand and buyers are assured that branded products continue to conform.

A.8 Test Laboratories

In support of an application to brand a product, X/Open requires among other things, a formal test report in respect of components for which a test tool is specified.

There are two sources of test reports that may be used for branding:

1. X/Open recognised laboratories, which have been through a formal quality assessment procedure
2. other laboratories which have not been through a formal assessment procedure.

Recognised laboratories are required either to have been assessed directly by X/Open for the conformance of their procedures to ISO guide 25, or to have been accredited by a national or regional accreditation body for the conformance of their procedures to ISO guide 25.

ISO guide 25 is concerned with the repeatability and reproducibility of formal test procedures and therefore provides X/Open and the branding programme with a firm foundation of

dependable test reports.

The alternative approach of non-recognised laboratories is dealt with by means of quality control rather than quality assurance. Branding applications through such laboratories are subject to a high percentage of random audit (the percentage varies between 80%-100% depending on the particular technology in question). This contrasts with the case of recognised laboratories which, in a low percentage of test reports, are subject to a technical audit (typically 5%).

A technical audit of the branded product is undertaken in a small percentage of cases, using the services of an independent third party test laboratory. Such an audit takes place in approximately 5% of branding applications, irrespective of the type of test laboratory that produced the original test report.

The audit rates quoted above are provisional and subject to review (up or down) in the light of our continuing experience of the branding programme. This policy applies equally to X/Open shareholders and non-shareholders.

A.9 Trade Mark Licence Agreement

The Trade Mark Licence Agreement (TMLA) is the primary governing document for branding and provides the legal enforcement of the conditions of the X/Open branding programme. Trade mark law provides the legal basis of this agreement. Under the conditions of the TMLA, a vendor warrants that its product does in practice conform to the specifications for which conformance is claimed. It requires specific evidence of conformance, such as test suites, where such test suites are available.

The TMLA imposes strict obligations on vendors for ensuring continuing product conformance, including:

- Specifications and test suites could never hope to be perfect or exhaustive. If a branded product is subsequently found to be non-conformant in some area by anyone making use of the product, the TMLA enforces the requirement on the vendor to make a publicly-available fix within a specified time.
- Products to which the licence relates may well include products from other suppliers. Responsibility for ensuring conformance however, remains with the branding applicant.
- In the case of a Profile Definition, the branding applicant warrants that all of the branded products that combine to implement the Profile, do work in combination, in practice. If problems happen to arise in connection with any of these products, it is the branding applicant's responsibility to ensure that they are resolved.

A.10 Profile Definitions

Certain Component Definitions may be combined together to support a specific functional need, such as a transaction processing system. These combinations of Component Definitions are called X/Open Profile Definitions and are meant to represent what the user actually needs to buy in practice.

There may be additional conformance requirements over and above those required by Component Definitions and individual specifications. If so, these are stated in the Profile Definition. However, in general, if a product or group of products conforms to each of the relevant Component Definitions, and also works together as a whole to allow applications to perform their tasks, it is conformant to the Profile.

A.11 In Summary

The X/Open Brand is much more powerful than most other certification programmes in that it delivers real assurance that the branded product purchased conforms to the relevant Component and Profile Definitions. In contrast, other certification programmes typically go no further than certifying that a particular configuration of a product on a certain day passed all the tests that were run against it.

When a product is registered as X/Open branded, the description and other relevant details are entered into X/Open Company's Register of Branded Products. This document lists all branded products and is a valuable reference tool for prospective purchasers who need to know what branded products are available on the market. X/Open distributes copies of this Register on demand.

In addition, each supplier who successfully brands a product receives a branding certificate which clearly identifies the product that is branded. Suppliers may use their certificates in their sales activities and promotional literature. Procurers may refer to them in order to make requirements statements concerning quality, portability and interoperability.

Appendix B

Rationale for Compilation of the XBSS Functional Components

B.1 Introduction

This appendix lists the various sources of the XBSS functional components and provides a rationale for their inclusion, or in a few key areas, their exclusion. Three sources of inclusion and one area of exclusion are addressed; they are as follows:

- *the Federal Criteria for security functionality*
- *the Federal Criteria assurance requirements for security manuals*
- *commercial user requirements for administrative roles*
- *commercial user requirements for secure networking.*

This appendix also provides a summary, tabular comparison of the XBSS functional components with the Federal Criteria sample commercial Protection Profiles and discusses differences between the XBSS and the TCSEC C2 functions and the ITSEC F-C2 functions.

B.2 The Federal Criteria Functionality Requirements

This section analyses the rated functional components of the Federal Criteria and details the rationale for the selection of the particular levels for each component. It explains why it was found necessary to select different levels for different components and why it was necessary in some cases to add, delete or modify some of the component primitives.

The rationale for the creation of a new X/Open protection profile rather than use an existing example was explained in detail in Section 3.2.3 on page 12.

B.2.1 Interpreting and Refining the Primitives

The process of collecting and interpreting or refining the primitives of security functionality components to create a security profile follows the concept of Protection Profiles. Selections of security functionality (and assurance, if appropriate) are extracted from Chapter 4 of the *Federal Criteria (FC)* and ‘‘interpreted’’ for the target usage environment or market segment. The interpreter is not restricted to the exact words of the Federal Criteria primitives and may add extensions/enhancements or delete unwanted sections. The primitives should not be reproduced verbatim but should be interpreted and elaborated upon so that no ambiguity or need for further interpretation remains.

Simple examples are that e.g.s be changed to i.e.s; that the requirement for defaults be replaced with the definition of specific defaults. Precisely such interpretation can be studied in the *Federal Criteria* sample Protection Profiles, CS1 through CS3 and LP1 through LP4. In these sample profiles, the difference between the primitives from the Federal Criteria chapters 4 and 5 and the Protection Profiles are highlighted in italics and in many cases the embellishment of requirements is significant.

Furthermore, the XBSS functionality is restricted to that which can be readily provided by vendors within a year of publication, leaving functions that have some implementation difficulty to be reconsidered at a later date. See Appendix C on page 61.

This section considers each area of security functionality, discusses the options available for the XBSS and derives a rationale for the choice made for the XBSS specification. Also mentioned are any functions (such as support for alternative authentication mechanisms from I&A-4) which are candidates for review at a later date. Preparatory work on an extended XBSS specification is an on-going effort. More information on XBSS development may be found in Appendix C on page 61.

B.2.2 Identification and Authentication (I&A)

The I&A-3 primitives from CS2 provides the most appropriate base for the XBSS, since both I&A-1 and I&A-2 are inadequate.

I&A-1 is inadequate because it doesn't include the ability for the system to determine security policy based on user attributes such as group affiliation. I&A-2 is inadequate because it has no requirement for the control of multiple login attempts.

Authentication mechanisms from I&A-4 are considered highly desirable but given the burden this would place on some suppliers, this requirement is postponed until later.

Other extensions to I&A-3, such as the use of ''only logging in using documented interfaces'' and ''requiring user accounts to have unique identities'', leads to the identification of this requirements as I&A-3+.

B.2.3 System Entry (SE)

A subset of the SE-1 items form the basis of of the XBSS. The requirements to grant entry in accordance with authenticated user policy attributes (SE-1 item 3) and for administrators to be able to modify and display these attributes (SE-1 item 4) are considered excessive for basic security and are not included in the XBSS. However the item to support user-initiated locking of the display screen (from SE-3) is considered to be part of basic security and is included. Items from SE-1 and SE-2 presently omitted in the XBSS are candidates for a later issue. Note that the commercial profile CS2 draws from SE-2.

B.2.4 Trusted Path (TP)

This is included in CS2 & CS3 as requirement TP-1. It was part of the TCSEC B2 requirements. However, this requirement is difficult to provide for all terminal types and its inclusion would disqualify a large part of the market. Less significant but pertinent, it has been suggested that only a knowledgeable and determined hacker would be capable of implementing a spoofing mechanism to exploit the absence of a trusted path and the XBSS has no objective to protect against such threats.

Future Direction

Trusted Path is not required in the XBSS, but is recommended as a candidate for a later issue.

B.2.5 Audit (AD)

AD-2 states auditing requirements comprehensively but goes beyond what would intuitively be expected for minimum commercial requirements in two out of five areas. A revised set of AD-2 primitives consistent with commercial XPG4 systems has been adopted for the XBSS. CS2 draws on AD-3 primitives. From AD-3 the *post collection analysis tools* should be considered as candidates for a future release of the XBSS.

B.2.6 Access Control (AC)

The functionality component AC-1 has a good basic set of primitives except that the requirement for controls of encapsulated objects is beyond the scope of the XBSS.

A shortened AC-1 is selected for the XBSS, with an import/export addition from AC-2. AC-2, revised to deal with wording difficulties with object sharing and propagation of access rights, is a candidate for a later issue. AC-2 is already used by CS2.

B.2.7 Resource Allocation (AR)

The XBSS systems will not attempt to address any denial of service attacks. Few implementations today support the requirement nor could they be implemented within a reasonable timeframe. The COFC has no requirement.

Future Direction

Resource Allocation is not required for the XBSS. It may be a candidate for a later issue.

B.2.8 Security Control - Based on FC Security Management (SM) and Privileged Operation (PO)

The SM-2 functional component with some deletions and additions from SM-3 is the most appropriate for commercial XPG4 compliant systems. Requirements on availability policies are considered out of scope for XBSS. The examples on password policies are fully covered in Section 4.4.5 on page 23, which is devoted entirely to password management. The examples of security policy attributes are informative and not normative and are moved to the Description and Rationale. Finally the sections from the SM-3 functional component on disabling and re-enabling of inactive user accounts is considered appropriate for commercial XPG4 systems and is included.

The functional component PO-1 is included with this section on Security Control, because privilege is at the heart of the requirement for administrative roles, which are considered critical for the security of commercial XPG4 compliant systems.

The SM-2 deletions and the remaining SM-3 requirements are candidates for a later issue.

B.2.9 Reference Mediation (RM)

CS1 and CS2 both use RM-1. However, the need to explicitly and separately state requirements for reference mediation seems excessive for the XBSS since the requirement is well represented under Access Control.

Future Direction

No separate requirement is needed for the XBSS. The notion of non-circumventability of security mechanisms has been added to individual functional components where appropriate.

B.2.10 TCB Protection (P)

The *Federal Criteria* for basic TCB isolation specifies a particular architecture, including its own domain, isolation of privileged and unprivileged address spaces, control of transfers between TCB and non-TCB domains, validation of passed parameters and many other architectural features. The X/Open approach expects that the XBSS requirements will be met as defined, in which case the Federal Criteria TCB architecture is just one choice for implementation. There are other architectures that may also meet the requirements.

Future Direction

Architecture for implementing the XBSS requirements will not be defined by the XBSS.

B.2.11 Physical Protection (PP)

For baseline commercial security, the physical control and protection of IT resources is an administrative responsibility and does not result in any software or hardware requirements.

Future Direction

The XBSS will not include specifications for Physical Protection.

B.2.12 System Self Checking (SC)

This item is considered to be the responsibility of the hardware platform supplier. Since it is an objective of X/Open security branding to be applicable to software products, independent of any hardware platform on which they might run, this item is not included.

Future Direction

System Self Checking is not a requirement of the XBSS.

B.2.13 Trusted Recovery (TR)

It is essential for XBSS compliant systems to have documented procedures for recovery from system failures or other discontinuities, such as to minimise the compromising of resource protection mechanisms. TR-1 with some minor changes is suitable. TR-3 may well be used at a later date.

B.2.14 Privilege Associated with TCB Functions (PO)

It is widely recognised that the structure of system privileges (where you either have super-user privilege and control over everything or user privilege and control only over your own resources), makes it necessary for strict security management practices to be enforced or risk potentially disastrous break-ins. The overhead of planning for and administration of these practices is considered too costly by a majority of potential commercial users of the system. These users require the identification of administrative functions and the assignment of minimum privilege roles to the performance of these functions. The direct use of super-user privileges must never be allowed for administrative purposes once the system is installed. Federal Criteria functional component PO-1 addresses this requirement and is therefore included in the XBSS in Section 4.8.6 on page 41 under the Security Control component.

B.2.15 Ease of Secure Use (EU)

Ease of secure use is a high priority for all security conscious vendors, buyers and users. However, the *Federal Criteria* primitives EU-1 through EU-4 are primarily a hierarchy of requirements for secure defaults for administrative functions and policy attributes for users, objects and services. The XBSS addresses default requirements with specific examples as part of the functionality requirements and not as a separate general topic.

Future Direction

The Federal Criteria EU-2 requirement for security service API's is well appreciated but is currently still undergoing standardisation as the IETF's GSS-API and is inappropriate for the XBSS but is a candidate for a later issue.

B.3 Security Manuals

The requirement for security manuals is derived from the Federal Criteria assurance requirements, UG-1 for the User Guide and AG-1 for the Basic Administrative Guidance. Similar requirements may be found in the TCSEC and the ITSEC.

B.4 Administrative Roles

Analysis of commercial user requirements indicates clearly that the uncontrolled use of full administrative privileges for all administrative activities is a serious security exposure and is unacceptable. Separate administrative activities must be identified and administrative roles assigned to perform these activities with the minimum of privilege for each role must be provided.

B.5 Secure Networking

Three topics of functionality have been analysed for the XBSS: non-disclosing authentication between communicants, data confidentiality and data integrity on data exchange.

Ensuring the confidentiality of the transferred information (protection from eavesdropping) is not included because of the unresolved export issues surrounding data encryption.

Ensuring the integrity of the transferred information is not included because even though message integrity, through the use of message authentication codes (MAC), is not covered by export restrictions, the MAC value needs to be protected from tampering, which does require some form of encryption, satisfactory solutions for which are not widely in place. Thus message confidentiality and integrity functionality, though recognised as known requirements with restricted solutions, have sufficient difficulties and a lack of international standard protocols associated with them to be omitted from the XBSS and to be included as candidates for a later issue.

Thus, non-disclosing authentication of the communicating users is the only requirement deemed practical, however known support for this function would be at the application layer using GSS-API. The real problem at the system level lies with the security of TCP/IP which is being addressed by the Internet Engineering Task Force (IETF) standards work and is therefore out of scope for the XBSS for the time being.

B.6 Comparison of Protection Profiles and Functionality Classes

This section summarises the XBSS in tabular form, identifying the Security Components using the labels employed in Chapter Four of the *Federal Criteria.*

It compares the XBSS with the sample commercial protection profiles, CS-1, CS-2 and CS-3 of the *Federal Criteria.* It also compares the XBSS with the TCSEC C2 and ITSEC F-C2 functionality classes. Note that XBSS(++) is a tabular listing of proposed candidate components and is not a commitment by X/Open to either support an XBSS(++) profile or an indication of its final contents should it be supported.

The rationale for the selection of a new X/Open Protection Profile is presented in Section 3.2.3 on page 12. The rationale for the selection of the set of functional components and their rating level, together with additions, deletions and modifications, is presented in Appendix B.

B.6.1 Comparison with FC

The following table presents the XBSS and XBSS(++) in terms of the Federal Criteria rated security functional components (for example, I&A-3, SE-1). They are compared with the Federal Criteria Protection Profiles CS1, CS2 and CS3.

The single plus "+" notation indicates that one or more primitives or parts thereof have been borrowed from the next level in the functional component hierarchy. The "r" notation indicates that some revision of wording of some of the primitives comprising the indicated level of the functional component is necessary.

The rationale for the "+" and "r" modifications to some of the selected functional components is presented in Section B.2 on page 53.

Security Component	CS1	CS2	CS3	XBSS	XBSS(++)
I&A	I&A-1	I&A-3	I&A-4	I&A-3+	I&A-4
System Entry		SE-2	SE-3	SE-1+	SE-3
Trusted Path		TP-1	TP-1		TP-1
Audit	AD-1	AD-3	AD-3	AD-2r	AD-3
Access Control	AC-1	AC-2+	AC-2+	AC-1r+	AC-2r
Resource Allocation			AR-1		
Security Management		SM-2	SM-3	SM-2+	SM-4
Reference Mediation	RM-1	RM-1	RM-1		
TCB Protection	P-1	P-1	P-1		
Physical Protection			PP-1		
Self Checking	SC-1	SC-2	SC-3		
Startup and Recovery		TR-2	TR-3	TR-1r	TR-3
Privileged Operations		PO-1	PO-2	PO-1*	PO-1*
Ease of Secure Use		EU-2	EU-3		

Table B-1 Comparison with FC

Note that with regard to the proposed candidate components for XBSS(++), Section B.2 on page 53, includes the rationale for the choice of components.

Note also that for the XBSS, PO-1* exists within SM-2+, the Security Management component.

B.6.2 Comparison with TCSEC C2 and ITSEC F-C2

The XBSS goes beyond C2/F-C2 security functionality in four areas. The XBSS includes requirements for administrative roles and security management (or control), which C2/F-C2 do not. The XBSS uses more evolved levels of I&A and Audit.

A not so obvious advantage of the XBSS is that it excludes those aspects of TCSEC C2 functionality evolved for military or intelligence applications but not required for commercial use. For example, TCB isolation architectures are left to the supplier and the reference monitor requirement is integrated into the other requirements by stating that key mechanisms must not be circumventable. F-C2 has no such architectural requirements.

Appendix C

Other Security Issues

This appendix explains X/Open Company's position on all high priority business requirements not addressed by the XBSS normative section. X/Open understands and accepts these requirements and will address them as far as possible within the scope of X/Open work. This appendix points to other X/Open work in progress (such as that in the System Management working group) which covers management and administration requirements rather than security requirements. This work will produce specifications in a reasonable time-frame which a future release of XBSS will be able to reference.

Work in progress by the System Management Working Group should lead to functionality which, if adopted by vendors, will reduce the costs of maintaining open systems. See Backup and Restore, below.

C.1 The Problem of Secure Networking

X/Open can only brand using agreed published standards. In the area of secure networking there is no such published standard to brand against.

- Wide area networks cross national boundaries, yet there is no agreed International Standard for secure networking.
- Work on securing TCP/IP is being carried out by the IETF (Internet Engineering Task Force) but the final strength of TCP's security is an unknown quantity.
- Confidentiality depends upon encryption, yet the use of encryption techniques for international data transfer is severely hampered by various governmental restrictions.

Whilst X/Open has not been able to provide as much as it would have liked in the area of networking, the reasons are outside its control. However, it is expected that the current situation will be resolved in the future.

C.1.1 Other Security Resources

The XBSS is not a complete solution to an organisation's security requirements. This section lists references which complement this specification.

- To effectively deploy security within an organisation, technology should be coupled with organisational procedures. A draft international standard has been published by ISO (ISO/IEC DIS 14980),[5] originating from the UK government Department of Trade and Industry Code of Practice for Information Security Management (British standard BS7799). The Code of Practice is based on a compilation of the best information security practices in general use in many leading international companies. The reports describe recommended procedures for implementing a security policy within an organisation, in order to facilitate secure links between the elements of trading partnerships.

  The services defined in XBSS support implementation of the Code of Practice.

5. See the Referenced Documents section at the beginning of this document.

- It is important to realise that, in spite of vendors' best efforts, security vulnerabilities are still likely to be discovered during the lifetime of a product and such vulnerabilities may be in functions not covered by the XBSS. Many vendors provide a ''security alert'' service, by which problems can be notified and fixes provided in a timely manner.

  Security alerts are also coordinated by independent national and international organisations, such as CERT (Computer Emergency Response Team) in the USA. The umbrella for these organisations is FIRST (Forum of Incident Response and Security Teams), which is located in the National Institute of Standards and Technology in Gaithersburg, MD, USA. FIRST is contactable via Internet electronic mail at `first-sec@first.org`; they will be able to direct you to the appropriate national organisation. There is also a World-Wide-Web home page at: `URL http://csrc.ncsl.nist.gov/first/`.

- Although XBSS does not (yet) address network security, there are a number of useful references which can assist in configuration of Internet-connected UNIX systems, in areas such as the setting up of anonymous ftp service. Information is available both in commercially available books and academic papers.

  Many papers are available on the Internet. A comprehensive and useful starting point is *Improving the Security of your UNIX System* by David A. Curry of SRI International. This is available from CERT via ftp at:
  `URL: ftp://ftp.cert.org/pub/info/security-doc.txt`

C.2 Audit Event Management / Security Event Detection

The business world's need for unique user identities is satisfied at baseline level by the XBSS in the requirement section on role-based access and privilege.

However, the XBSS cannot prevent bad management practice. An example of this is where one person, *userA*, makes a habit of logging into different consoles. Since *userA* cannot be in two places at once, an impostor can use the unattended terminal and do much damage if *userA* has wide-ranging access privilege.

The XBSS does not provide the event management which could detect the security anomaly just described. The record of erratic behaviour would exist in the audit trail, but no alarms would be raised.

X/Open has scheduled work on Security Event Detection (Intrusion Detection) and results of this work will be incorporated into a future release of XBSS.

C.3 Backup and Restore

The provision of backup and restore facilities in a system presents several security concerns in respect of both confidentiality and integrity. These concerns are partially addressed in this specification by the requirement for separable administration functions for backup only, and for the combination of both backup and restore.

There is scheduled work for a project on *Secure Backup and Restore* and therefore in future the security brand is likely to include further functionality.

Vendor documentation should either assist users in this area or suggest further reading (for example the Administrative documentation) so that they might be encouraged to use the correct working procedure for making secure and cost-effective backup.

It should also be noted that where the security brand is associated with the XPG4 Base or Single UNIX specification, those specifications also include requirements on backup and restore facilities.

C.4 Special Interpretations for the UNIX Operating System

X/Open acknowledges that a UNIX system specific interpretation of XBSS would be extremely useful. It is in such a section that details of the initial ‘‘out of the box’’ settings for key control files can be discussed and defaults given. At present there is no commitment or schedule for performing this work.

C.5 Single Logon Facility

Single Log-on implies an open distributed environment that supports a single system image. At the present time, this is out-of-scope for the XBSS, but may come into scope as distributed systems evolve. Single logon is likely to be a scheduled project for X/Open in the future.

C.6 Simplifying Security Administration

Vendor documentation should give a high level of priority to explaining the security required for the installed system. If users need high security they should be shown how to achieve it. The provision of default parameters and easily selected optional parameters will enable a security conscious site to quickly achieve their appropriate level of security. A good level of security which is held in a robust state by easily-administered maintenance programs will, in itself, reduce the costs of security administration. The XBSS addresses administration in Section 4.8.6 on page 41.

C.7 File and Record Locking

File and record locking is provided by standard interfaces in the *Common Applications Environment System Interfaces and Headers of XPG4*, Version 2. There are many branded products already available.

Appendix D

Acknowledgements

D.1 The European Security Forum

The European Security Forum has been a valuable partner to X/Open in its development of the X/Open Baseline Security Services. In particular, the European Security Forum's UNIX Security SIG has reviewed the developing XBSS in detail and has contributed much in the way of detailed comment and user perspectives to the X/Open Security Working Group.

X/Open would like to thank the members of the European Security Forum, in particular the members of the ESF UNIX Security SIG for their contribution. The members of the SIG were as follows. Alan Stanley and Marco Kapp were the project leaders.

European Security Forum UNIX Security SIG			
Members	*Representing*	*Members*	*Representing*
John Brophy	AIB Group	Julie Wilkerson	Mercury Communications
Michael Hanna	Bank of Ireland	Brian Christie	National Power
Joy Bateman	Barclays Bank	Steven Dixon	Nationwide Building Society
Walter Reynolds	Barclays Bank	Alistair MacWilson	Price Waterhouse
David Slade	Bellcore	Chris Lomax	Racal Datacom
Jason Creasey	BOC Group	Jeremy Turner	Rover Group
Rob O'Neill	British Aerospace	Andy Haxby	Shell Common Information Services
Martin Taylor	SIG Chairman	British Airways	Brian Hickey
Edward Evans	British Gas	John Jones	Shell Common Information Services
Kath Bees	British Steel	Dio Koolen	Shell International
David Jones	Cadbury Schweppes	Jerry Janzen	Shell International
Alan Stanley	ESF Management Team	Billy McConnell	Ulster Bank
Steve Thorne	ESF Management Team	Maggie Richens	Zeneca Computing & Telecommunications
Ian Gale	Ford Motor Company	Paul Hibbert	Zeneca Pharmaceuticals
Marco Kapp	Kapp & Partners		

The full membership list for the ESF (for November 1995) is given overleaf.

European Security Forum			
Organisation	*Country*	*Organisation*	*Country*
An Post	IE	Johnson & Johnson	US
AIB Group	IE	KPMG	GB
ASTRA	SE	Kredietbank	BE
Bacob Savings Bank	BE	La Poste	FR
BACS	GB	Lloyd's of London	GB
Bank of Ireland	IE	Marks & Spencer	GB
Bank of Scotland	GB	Mercury Communications	GB
Barclays Bank	GB	Ministerie van Financien	NL
BASF	DE	National Power	GB
BAT Industries	GB	National Westminister Bank	GB
Bayer	DE	Nationwide Building Society	GB
The BOC Group	GB	Nestle	CH
The Boots Company	GB	Nuclear Electric	GB
British Aerospace	GB	Paribas Capital Markets	GB
British Airways	GB	Philips Communications	NL
British Gas	GB	Pilkington	GB
British Steel	GB	Post Danmark Informatikservice	DK
British Telecommunications	GB	The Post Office	GB
Cadbury Schweppes	GB	Price Waterhouse	DE
CEDEL	LU	Prudential Assurance Corporation	GB
CETREL	LU	PTT Telecom	NL
Christiania Bank	NO	Racal-Airtech	GB
Citibank	US	F Hoffman-La Roche	CH
Civil Aviation Authority	GB	Rover Group	GB
Coopers & Lybrand International	GB	Royal Bank of Scotland	GB
Credit Suisse	CH	J Sainsbury	GB
Daimler-Benz	DE	Sandoz International Ltd	CH
Den Norske Bank	NO	J Henry Schroder	GB
Department of Social Welfare	IE	Scottish Hydro-Electric	GB
Deutsche Telekom	DE	Scottish Nuclear	GB
Digital Equipment	GB	SDC	DK
Electricity Supply Board	IE	Shell Common Information Services	NL
Eurocontrol	BE	SKF	SE
Europay International	BE	South African Mutual Life	ZA
LM Ericsson Data	SE	Standard Life	GB
Ford Motor Company	GB	Sun Alliance Group	GB
GE Capital Global Consumer Finance	GB	S.W.I.F.T.	BE
General Accident Fire & Life Corp	GB	Swiss Bank Corporation	CH
Generale Bank	BE	Telecom Eireann	IE
Girobank	DK	Telia	SE
Gjensidige	NO	Union Bank of Switzerland	CH
Glaxo Wellcome	GB	Vaerdipapircentralen	DK
Guinness	GB	Volvo Data	SE
Halifax Building Society	GB	SBC Warburg Group Management	GB
		Zeneca	GB

Special status members:	Bank of International Settlements (observer)	(CH)
	Bundesamt fur Sicherheit in der Informationstechnik	(DE)
	Department of Trade and Industry	(GB)

D.2 The Security Requirements Topic Group (SecRTG)

X/Open also acknowledges the work of the Security Requirements Topic Group (SecRTG), in particular Peter Shuttleworth of the UK Ministry of Defence, Jeremy Hilton of ASE Consulting, Nick Mansfield of Shell International, Karen Worstell of Boeing, Dick O'Donnell of Harris Corporation, Mark Andrews of Electronic Data Systems, Terry Brookman of Barclays Bank and Jim Keithley of Guide International.

The membership list for the SecRTG is shown here.

X/Open Security Requirements Topic Group			
Members	*Representing*	*Members*	*Representing*
Rene J Aerdts	Technology Management	Stephane Martinez	Elf Aquitaine Production
Jan Andersson	Sweden Post	Larry McCaffery	DSS-ITSA
Tom Anderson	Tandem	Piers McMahon	ICL
Mark Andrew	Electronic Data Systems (EDS)	Jon Measham	UK Post Office
Tom Arnette	PRC Inc	Michel Mercier	Electricite de France / DER
David Aucsmith	Sequent Computer Systems Inc	Roger Merckling	HP
Ian Baker	CCTA	Chris Milsom	Novell
Ian Baker	CCTA	John Minter	Inland Revenue
Barry Barber	NHSIMC	Cyril Murphy	MITRE Corporation
David Blair	DSS-ITSA	Richard Murphy	Amdahl
Kevin Brady	Novell	Yasushi Nakahara	Toshiba
Terry Brookman	Barclays	Craig Newmark	Schwab
Peter Callaway	IBM	Dick O'Donnell	Harris Corporation
Miguel Caputi	Bull	Jeff Picciotto	MITRE Corporation
Shu-jen Chang	NIST	Denis Pinkas	Bull
Francoise Chevalier-Goffe	Electricite de France	Bob Pritchard	Gradient Technologies
Brian Dear	BarclaysBank	E Reeh	AT&T
Philippe Decottignies	HP	Amy Reiss	NSA
Belinda Fairthorne	ICL	David Rogers	OpenVision
Kenneth J Gaertner	NCSC	Craig Rubin	Novell
Frederic Gittler	HP	Nigel Salt	CCTA
Dave Gomberg	Mitre Corporation	K Sastry	DEC
Maria Teresa Grilo	CSELT / STET	Janice Schafer	DISA
Henry Hall	DEC	Fritz Schulz	NIST
Suri Harish	Tandem	Hans-Juergen Seidel	SNI
J Reed Harrison	Harris Corporation	Peter Shuttleworth	Ministry of Defence DGITS
Reed Harrison	Harris Corporation	Bill Smith	DISA
Craig Heath	SCO / IXI	Don Stephenson	SUN
Jeremy Hilton	ASE Consulting	Julie A Surer	MITRE Corporation
Bertil Holmqvist	TeliaAB	Haruki Tabuchi	Fujitsu
Anne Hopkins	HP	Hideo Takahashi	Hitachi
Martin Jess	AT&T	Masanori Tanaka	Fujitsu
Don B Johnson	IBM	Lutz Temme	SNI
Martyn Joyce	Amdahl	Philippe Thomas	Banque Nationalde Paris
Jim Keithley	Guide International	Wolfgang Tietz	Bundesamtfur Informatik
Chip Kerr	Electronic Data Systems (EDS)	Jeff Tonkel	Tandem
Samir Khlif	HP	Peter Trachsel	Bundesamt Fur Informatik
Bob Kruger	Microsoft	David Willis	Bull
Ellen W Law	DISA	Gary Winiger	SUN
Yves LeRoux	EUROBIT	Karen Worstell	Boeing
Hugo Lunardelli	Microsoft	John Wray	DEC
Ruaridh MacDonald	UK Ministry of Defence	Ken Zemrowski	TRW Systems
Rhonda MacLean	Boeing	Rainer Zimmer	SNI
Nick Mansfield	Shell International		

D.3 SWG XBSS Project Team

X/Open gratefully acknowledges the work of the following members of the XBSS Project Team of the X/Open Security Working Group (SWG) in the preparation of this document. The XBSS Project leader is Peter Callaway.

X/Open Security Working Group			
Members	*Representing*	*Members*	*Representing*
Dave Bauer	Bellcore	Piers McMahon	ICL
Kevin Brady	Novell	Sven Munther	AT&T
Joe Brame	Unisys	Richard Murphy	Amdahl
Peter Callaway	IBM	David Rogers	OpenVision
Frederic Gittler	HP	Hans-Juergen Seidel	SNI
Craig Heath	SCO	Don Stephenson	Sun
Ingo Hoffmann	SNI	Brian Weis	Amdahl
Anne Hopkins	HP	David Willis	Bull
Jim Keithley	Guide International	Gary Winiger	Sun

Appendix E

Some Terms Explained

E.1 The Meaning of the Term ′user′

In the description of the security functionality primitives, which starts with Section 4.4.1 and continues until Section 4.10.2 the term *user* should be taken to mean a *registered* and *authenticated* user of the system. A registered user is a person known to the system and having a number of properties declared within the system's user database. These include *login name*, *user ID* (UID), *group ID* (GID), *initial working directory*, and *initial user program*. An authenticated user is a person recognised by the system as having successfully fulfilled a stringent login procedure. A *password* checking routine is usually associated with the login procedure. For further technical explanation of these terms, refer to chapter 2 of the **X/Open Security Guide**.

Most information technology (IT) systems will have many *normal users* who, once authenticated, are authorised to use a limited part of the system. There may also be one or more *administrative users*, who have access to a greater number of directories and who have read, write and execute permission on a large number of files.

Root

By historical circumstance there is one category of user who possesses the highest level of authorisation. This is the **root** user who has **super-user** privilege. The account for **root** gives the highest level of privilege and any user who can successfully perform *$ /bin/su - root* can effectively by-pass most security checks on the system.

For the correct interpretation of the XBSS security functions it is vital that the use of **root** is limited to a known administrative user and that this user's use of **root** follows the guidelines explained in the section on the **super-user** in chapter 6 of the **X/Open Security Guide**.

Non-human Users

root is not a human user of the computer and is known as a *pseudo-user*. There are other pseudo-user accounts besides **root**, but these do not necessarily have super-user privileges. Therefore the term ''user'' includes both persons and inanimate mechanisms. This chapter makes no distinction between *pseudo-user*, *super-user* and *user*. They are all simply *users*. Human users should be discouraged from logging in by a non-human username since to do so would be to defeat accountability. However, the use of *su(1)* to enter a non-human or ''role'' username is permissible since it preserves accountability.

How This Document Uses The Word User

Where the text requires a more accurate description of a user, then the term *normal user* or *administrative user* is used.

Finally, in referring to the term *user*, *normal user* and *administrative user* the male gender is used for stylistic purposes, since the form of wording needed for a genderless description of *user* would render the functional descriptions less precise and so open to misinterpretation.

E.2 The Terms ′protected mechanism′ and ′uncircumventable′

The *Federal Criteria* uses the term *protected mechanism* to refer to a collection of procedures and data objects in a secure subsystem. In the domain thus created any data object is accessible only to a procedure held in the subsystem. The procedure can only be called through designated domain entry points.

Protected mechanisms should be provided to handle the requirements of any particular security procedure, which in itself should be meticulously defined and not open to misinterpretation or imprecise usage. In particular it should not be possible for a user or entity to evade any of the security mechanisms which are in place, either accidentally or by a wilful attempt to by-pass a security procedure.

Effective security is only made possible by the provision of mechanisms which are said to be *uncircumventable*. An uncircumventable mechanism may enforce a security policy such as the validity of the login session, or it may protect security tools such as the audit trail facility. However, it should be recognised that in terms of the XBSS specification the term *uncircumventable* is not an absolute. A computer-based process controlling the security functions of an IT system in a non-military installation, as represented by any contemporary industrial or business organisation, may not in truth be wholly uncircumventable. The intent is that the protected process be as uncircumventable as is possible without recourse to an unacceptable degree of security barriers.

E.3 Interconnected Homogeneous and Distributed Heterogeneous Systems

- *interconnected* — a possibly heterogeneous network of systems, running a variety of applications which are not required to co-operate as a single coherent business application. These applications may require such facilities as: common remote file server, file transfer, email-type message transfer, remote login capability. In general, they require some network communications security support.
- *distributed* — an environment that supports communicating, co-operating applications on different systems across a network, to allow the individual applications to function together as a single coherent business application, distributed across the network. In general, these applications require application or platform service security support for application to application interworking.
- *homogeneous* — a network consisting of computers of the same type.
- *heterogeneous* — a network consisting of computers of varying types.

E.4 Glossary

For common computing terms refer to the glossary in the **Procurement Guide**.

access control
A control mechanism whereby a *subject* is given no access, limited access or full access to an *object*.

access control attribute
Subjects and objects have attributes which are used to determine the accessibility of the object by the subject.

The access control attributes of subjects are at least: named users, the effective and real user ID of the subject, named groups, the effective and real group ID of the subject and the supplemental groups of the subject.

The access control attributes of objects are at least: read, can read data and view attributes, write, can write data and modify attributes, execute, can execute the contained program, or search a directory.

administrator
A trusted user, authorised to perform system management and maintenance functions essential to the smooth and secure running of the system. These functions are not available to the general user either through a privilege mechanism whereby general users have one privilege and the administrator another or through the use of special login identification.

administrative user
A user who has been authenticated to an IT system and who has authorisation to perform tasks which a normal user would not be allowed to do. An administrative user would have the authority to perform administrative functions and would be able to change the functioning of any part of the system which pertains to security policy.
See also *normal user*.

audit
A security audit is an independent review and examination of systems records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security and to recommend any indicated changes in control, policy and procedures.

audit trail
Data collected and potentially used to facilitate a security audit.

authenticate
To establish the validity of a claimed identity.

authorised user
A user who has been authenticated to an IT system and has been granted rights of access to system resources based on the user's policy attributes.
See also *normal user*.

The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)
The CTCPEC was derived from the US TCSEC to meet the needs of the Canadian Government and recognised the need to address data integrity and resource availability as well as data confidentiality. In the ongoing work to harmonise the various criteria programmes, the CTCPEC authors worked with the authors of the Federal Criteria and later the Common Criteria to achieve an internationally acceptable standard.

Commercially Oriented Functionality Class (COFC)
At the same time that the ITSEC and the Federal Criteria were being developed, ISO was working toward an International Standard for Evaluation Criteria. The ISO proposal called for classes of security functionality to be submitted by authoritative bodies for selected market segments. ECMA, the European Computer Manufacturers Association submitted such a standard class with the COFC. The COFC was largely derived from the MSFR, but was simplified and generalised. Future versions of the COFC were planned but nothing was produced. One might expect that the COFC would be converted to a Protection Profile for commercial use, once the Common Criteria is completed and adopted by ISO.

Common Criteria (CC)
An international initiative to bring together all current criteria systems under a single programme. Mutual recognition of results is a major objective. At the same time investments in prior programmes will be preserved. The CC is being written by the Common Criteria Editorial Board, staffed by representatives from all countries that currently have their own native programmes, including Canada, France, Germany, the USA and the UK. The CCEB is backed up by teams of researchers and ongoing workshops to address and resolve problems of functionality and assurance for distributed systems. The first (incomplete) draft was published for review in December 1994.

European Computer Manufacturers Association (ECMA)
An association of companies and organisations, all of which are involved in the development, manufacture and marketing of hardware and software products or services in the IT field.

European Security Forum (ESF)
The Forum consists of representatives from major European IT organisations and is dedicated to clarifying and resolving key issues in IT security and developing security solutions that meet the business needs of its members.

Federal Criteria (FC)
A US initiative to combine the best features of the US, Canadian and European Community security evaluation criteria programmes and to advance the state-of-the-art to make criteria programmes more flexible for markets other than the military/intelligence and non-classified but sensitive. It defined security functionality components in terms of of a hierarchy of primitives derived from the TCSEC, ITSEC, CTCPEC, and MSFR, and represented the most comprehensive set available at its time of publication. It introduced the concept of Protection Profiles and thereby the ability of authoritative market segment representatives to define criteria combinations tailored to their market. This was in contrast to the single set of predefined bundles of functionality and assurance criteria as represented by the TCSEC.

International Information Integrity Institute (I-4)
I-4 draws its membership from Europe, USA and Japan. Information on security matters is shared through forums, publications and electronic communications.

initiator
An entity (for example a human user or computer based entity) that attempts to access other entities.

interconnected systems
Systems that are connected via telecommunication links and are capable of exchanging information using common communication protocols. Such systems may not provide client-server or distributed computing facilities, they simply connect in order to exchange data.

The Information Technology Security Evaluation Criteria (ITSEC)
Since non-US products could not be evaluated using the TCSEC, several European Community countries co-operated in the development of a programme for evaluating secure systems or

products in Europe. The ITSEC focused primarily on developing assurance criteria and introduced the concepts of correctness and effectiveness and emphasised the need to address data integrity and resource availability as well as data confidentiality. The ITSEC allows a vendor to define its own set of security functionality (the Target of Evaluation or TOE), but provides sample sets of security functionality that correspond closely to the six TCSEC levels. For example F-C2 corresponds closely to the TCSEC C2 functionality criteria.
See also COFC.

login session
A login session starts when the when a user enters his identity to the system and completes authentication of that identity. A login session remains active until the user exits from the system terminating his interactions with the system. User-initiated locking and re-authentication may be considered the same login session relative to password criteria, or at the option of the vendor, to count as a new authentication for account locking or delaying and password expiration.

mechanism
A security mechanism is a supplier selected method for implementing a security function or algorithm.
See also *protected mechanism*.

The Minimum Security Functionality Requirements (MSFR)
This was the first attempt at a definition of commercial security requirements by representatives of the users themselves. Although eventually owned by NIST and merged in with the Federal Criteria, the origins of the MSFR was Bellcore and American Express with EDS. Bellcore produced the Bellcore Operations Systems Security Requirements while American Express Travel Related Services and Electronic Data Systems Corporation produced the Commercial International Security Requirements (CISR) which was adopted by I-4. NIST merged the two proposals with a view to creating a Federal Information Processing Standard (FIPS), but the FIPS was not published when the work was merged in with the Federal Criteria. Much of the MSFR can be found in the Federal Criteria, although somewhat reworded in many cases.

normal user
A user who has been authenticated to an IT system but who has no special authorisations. Such a user may only access those resources identified as under his ownership. This user should have no authority to perform administrative functions and should not be able to change the functioning of any part of the system which pertains to security policy.
See also *administrative user*.

normal system administration
Normal system administration is the day to day administration of the system. It is provided by, but not limited to, the functions specified in Section 4.8.6 on page 41. It includes functions that might reasonably be expected of day to day administration. It does not include functions that require maintenance mode or functions that would reasonably be expected to require special technical skills or training. Examples which may be considered neither maintenance mode nor normal system administration are restart of system daemons and installation of vendor supplemental, or third party software.

Note: Initial system installation is a maintenance mode operation.

object
A controlled entity that precisely gives or receives information in response to access attempts by another (active) entity. Also known as a target.

Orange Book
See TCSEC.

policy attribute
A security policy attribute is a piece of security information associated with an entity once it has been authenticated to a system. The information may be used to determine what resources the entity may be authorised to access on the system. When associated with an object, it may be used to determine what attributes must be associated with entities for them to be granted access to that object, e.g., entity name, group, role or modes of access.

principal
An entity whose identity can be authenticated.

protected mechanism
The *protected mechanism* of the TCB is a term that may be used interchangeably with *encapsulated subsystem* and *protected subsystem*. It refers to a collection of procedures and data objects that is protected in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected mechanism and that those procedures may be called only at designated domain entry points.
See also Section E.2 on page 70.

Protection Profile (PP)
A key concept introduced by the Federal Criteria and carried over to the Common Criteria. A Protection Profile describes, for a particular market segment, the security risks and exposures and identifies the security policies required to address those risks. It then selects the security functionality and assurance criteria appropriate for its market and provides a rationale for this choice. In selecting these criteria from the basic set of primitives, interpretation of these primitives for the target market environment is provided, in order to avoid ambiguity in understanding the requirements of the protection profile by vendors, users and evaluators.

pseudo-user
A non-human or anonymous user of the system.
See also Section E.1 on page 69, normal user and administrative user and the definitions for normal user and administrative user given in this glossary.

reusable password
Passwords are used to authenticate an entity that is attempting to identify itself so that it may gain access to controlled resources. A password may be used for a single authentication (after which it must be replaced with a new one) or it may be used for multiple authentications in which case it is known as a reusable password. Re-usable passwords usually expire after an installation defined period of time after which they must also be replaced with new ones.

session
A session is the execution of a series of programs on a system started on behalf of a user by a system facility. A particular case of a session is a 'Login Session'. Other types of session may be started by facilities which offer batch, scheduled, or delayed execution. A session exits when the last of the series of commands is executed.

subject
An active entity in an IT product, generally in the form of a process or a device, that causes information to flow among objects or changes the system state. Also called an initiator.

Trusted Computing Base (TCB)
The totality of protection mechanisms within an IT system. The definition normally includes the hardware element, hence; *Within the TCB a combination of hardware, firmware, software and data is responsible for enforcing the security policy*. In this document hardware platforms are not considered, so for this document the definition of TCB does not include the hardware element.
See also TCSEC and Section 3.4.2 on page 14.

Trusted Computer System Evaluation Criteria (TCSEC)
The TCSEC or Orange Book, published by the US Department of Defense in 1985. Focusing primarily on functionality and assurance criteria and security policies for the protection and confidentiality of classified data, it introduced the concepts of discretionary and mandatory access control using a reference monitor within the confines of a Trusted Computing Base (TCB). The TCSEC defines a hierarchy of six functionality and assurance classes of which the C2 level proved to be the most useful for commercial systems. The TCSEC lacked criteria for data integrity and resource availability.
See also COFC and MSFR.

Target of Compliance
Those components of a supplier's package, defined by the supplier as a specific subset of the total package, which will be subject to the X/Open security specifications.

Target of Evaluation (TOE)
An IT system or product which is subject to security evaluation.

uncircumventable
The property of a mechanism that cannot be by-passed when it must be used to enforce an installation security policy.
See also Section E.2 on page 70.

Index