INFORMATION SECURITY LABELLING
Requirements Statement

The Open Group Security Program Group

Version 7.2 September 1997

1. Introduction

This paper contains requirements for a standard on data labelling. The requirement is for a common interoperable label structure that can be associated with each information-containing object in an IT system.

The growth of the 'Information Society' has brought about a great increase in the sharing of sensitive information between organisations, including personal and financial details, Intellectual Property, issues of national security, and material not for viewing by minors. Security policies state how material is to be handled during storage, processing and transmission to maintain its security. Hard copy is said to carry markings while objects in IT systems carry corresponding labels, which indicate, in conjunction with a security policy, how sensitive material is to be handled.

The paper gives the scope of the proposed standard, states the business case for standardised labelling, states the requirements, and presents a roadmap outlining the action that needs to be taken. Some definitions are given in Annex A and background information on labelling is in Annex B. Annex C describes the use of labelling in different business scenarios.

This requirements document was approved by the Security Program Group at the Boston Members Meeting of The Open Group in September 1997, subject to reservations about the proposed roadmap until there is shown to be a demand for labelling from the marketplace.

2. Scope

This paper sets out the requirements for a standard defining the syntax of security labels. A label may be associated with each information-containing object in an IT system, such as documents, electronic mail messages, database entries, directory entries, electronic forms and packets sent over networks. Thus labels are not restricted to use with objects handled by users applications, but may be associated with objects used by any part of a communications stack or operating system. The labels are intended for use when objects are stored, transmitted between systems, and when they are being handled by applications that act on labels.

The security policies with which labels are associated are varied and include policies for confidentiality, integrity, for example. (These examples are not intended to be exclusive, and overlap.)

The following are outside the scope of the standard.

- The definition of security policies.
- Protocols for the communication and negotiation of security policies between systems.
- The semantics of labels (as these are determined by their security policies).

- The definition of mechanisms that make use of labels and enforce their semantics.
- The representation of markings on hard copy.

3. Business Case

The business benefits of labelling are:

- to support mechanisms controlling access to data according to its sensitivity;
- to support mechanisms controlling access privileges; and
- to reduce costs by avoiding the need to secure all data on a system to the level of the most sensitive.

The business benefits of a common labelling standard are:

- to facilitate secure systems interoperability;
- to reduce the costs of secure systems interoperability by avoiding the need for costly translators or gateways between systems;
- to reduce the risk of handling labelled material incorrectly;
- to avoid confusion with labels defined by other organisations;
- to reduce system administration, both in running a system and in upgrading it;
- to facilitate the portability of secure applications; and
- to facilitate interworking between different file types (e.g., in multi-media applications, embedding objects in others), as the same label syntax is used for each.

Various business scenarios are described in Annex C.

4. Requirements

A labelling standard shall be defined that is common across different vendor's platforms, applications and object types. The standard shall define the syntax of labels.

The labels defined by the labelling standard shall:

- identify uniquely the security policy that the label belongs to;
- be flexible to allow for changes to security policies;
- be extensible to allow new components of security policies to be added;
- allow new security policies to be defined;
- be bound logically to their associated objects such that only applications authorised by the security policy can remove or alter the label;
- support evolving data classification standards;
- support rules used to manipulate labels, such as downgrading; and
- support rules that determine the label to be applied to an object compiled from sources bearing different labels.

Labels shall be defined independently of:

- the objects to which they apply;
- the applications which create and use these objects, and how the applications are implemented;

- the means of storage or transmission of the objects, including communications protocols used to transmit the objects; and
- any specific business requirements of individual systems in which they are used.

The standard should address the use of labels at different layers in the communications stack. A security policy may, for example, place requirements on routing (such as preventing material with adult content from entering specified domains) or may require packet encryption. Thus labels may need to be passed between elements of the stack. However, the different constraints on different elements of the stack, such as whether encodings need to be kept small, may mean that different encodings are required.

5. Roadmap

Satisfying the requirement expressed here is only a first step towards the goal of making labels interoperable between systems. The roadmap below describes the further steps required.

In order to make progress on labelling standardisation, it needs to be taken in discrete stages, as follows. These activities do not need to be carried out sequentially, nor in the order shown. Not all of these stages needs to be complete before new product developments can take place. Several of these stages are described in more detail below.

1. Define a standard label syntax meeting the requirements above.

2. Define APIs for the handling of labels.

3. Define a business exploitation plan for the labelling standard, including a branding programme.

4. If necessary, set up a registration scheme for security policy identifiers.

5. Define a number of general security policies for use within specific groups.

6. Integrate labelling into Open Group education and training programmes.

Standard Definition. The Specification Working Group (SWG) will produce the standard. If an existing standard meets the requirements, this will be adopted. If an existing standard meets many of the requirements and can be adapted to meet the rest, this will be done. Only if neither of these approaches is appropriate will a new labelling standard be developed. The SWG and the existing Labelling Task Group will work together to ensure that the requirements are met in ways that the vendors can develop into commercially successful products.

Business Plan. The Security Programme Group will draw up a business exploitation plan for the labelling standard. The plan will consider who would be likely buyers of products that use the standard, and how best to ensure uptake of the standard. It is intended that the specification chosen or developed to meet this requirement should form part of an X/Open branding programme for products that guarantee to support the specification. Since the range of applications that are likely to make use of labelling is much wider than those that already form part of an X/Open branding programme, a new branding programme should be set up to deal with labelling.

Registration. It is expected that the label specification that satisfies the requirements given here will need to include an identifier for the security policy with which a label is associated. It is likely that such an identifier would include a reference to the organisation owning the security policy,

in which case it might be possible to use an existing registration scheme. Note that registration of a policy identifier (or set of policy identifiers) need not require the policy itself to be made public.

Policies. It is expected that different groups such as banks, Governments and the entertainment industry may wish to agree security policies appropriate to the bulk of communications within their group. Inevitably there will be some communications, perhaps those involving particularly sensitive information, that will not be included in such general policies. It is likely that the development of security policies will be considered to be outside the scope of The Open Group.

Annex A. Definitions

ACCESS CONTROL

The prevention of unauthorised use of a resource including the prevention of use of a resource in an unauthorised manner.

AUDIT

See SECURITY AUDIT

AUTHENTICATION

Verification of claimed identity.

AUTHORISATION

The granting of rights, which includes the granting of access based on access rights.

CONFIDENTIALITY

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

DATA INTEGRITY

The property that data has not been altered or destroyed in an unauthorised manner.

DIGITAL SIGNATURE

Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery for example, by the recipient

DOWNGRADING

Changing the label associated with data to reflect a reduction in the sensitivity of the associated information.

INTEGRITY

See Data Integrity.

.

SECURITY AUDIT

An independent review and examination of system records and operations 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.

SECURITY CLASSIFICATION

A set of information of a similar value, and degree and nature of sensitivity.

SECURITY LABEL

A machine readable representation bound to a resource (which may be a data unit) that names or designates the security attributes of that resource

SECURITY MARKING

A human readable word or phrase bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

SECURITY POLICY

The set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organisation.

SECURITY SERVICE

A service which may be invoked directly or indirectly by functions within a system that ensures adequate security of the system or of data transfers between components of the system or with other systems.

SENSITIVITY

A measure of importance assigned to information by the information owner to denote its need for protection.

Annex B. Background Information on Labelling

With the increasing use of information technology, the growth in electronic commerce, and greater outsourcing of services, there is a growing demand for the commercial, industrial, public and private sectors to work together and share information. This in turn has brought about a corresponding increase in the volume of proprietary or other sensitive information that is transmitted between organisations, both in hard-copy and electronic form. This information may include, for example, personal and financial details, marketing information, negotiating positions, research results, details of manufacturing processes and other Intellectual Property Rights, issues of national security, and entertainment material with violent or adult content not for viewing by minors. Severe damage or embarrassment can be caused to either the originator or holder of sensitive information if, for example, it is released to those not authorised to receive it (a breach of confidentiality), or if it is modified in any way (a breach of integrity). It is, therefore, becoming increasingly important that information in all forms is adequately controlled and protected during its storage, processing and transmission between and within organisations over both private and public networks.

Each organisation needs to draw up security policies to protect its sensitive information appropriately and cost-effectively. A security policy may express security requirements in terms of protection against:

- unauthorised disclosure (confidentiality);
- unauthorised changes (integrity); and
- protection against unauthorised copying by authorised recipients.

The security policy lays down how information is to be handled, by considering aspects such as:

- the level of protection to be given to data stored on a system;
- who is able to access it;
- the security markings shown on any display or print of the material;
- whether operations on the object are to be audited;
- the routing of data transmitted between systems, and whether it needs to be encrypted; and
- whether digital signatures are required to authenticate the data, and whose digital signature is required.

Note that confidentiality can include prevention of access to adult material by minors, and prevention of copying might be used to protect copyrighted material and other intellectual property.

The variety of protections that organisations might wish to express in a security policy and the number of ways these policy elements might be combined and varied cannot be entirely anticipated.

Each organisation will place assets of comparable value or requiring comparable protection into one of a set of predefined classifications according to the security policy. All assets given the same classification will be handled to provide them with a comparable level of protection. The names of the classifications are usually referred to as markings (or protective markings). Current usage describes hard copy as being ‘marked’ with the classification, while objects in IT systems are ‘labelled’. Thus hard copy carries ‘markings’ (or ‘security markings’) while objects in IT systems carry ‘labels’. Thus the marking or label associated with each asset indicates how the asset is to be handled (by reference to the security policy).

A label can be examined by IT systems and networks to make security-relevant decisions, such as on access control and on routing (e.g. choosing between a secure link, a standard dial-up line, or the Internet), without needing to access the information that is being protected.

Many security services make use of classifications. For example,:

- A database management system (an application) may associate classifications with fields, records and tables within the database.
- An operating system associates classifications with processes, files, and so on.
- A communication system associates classifications with messages and packets.

Without using a means such as labels to easily assess the sensitivity of the information involved, access mechanisms need to be secured to the level of the most sensitive information that is being accessed. Once a data labelling system is in place, costs can reduce, as 'strong' authentication, encryption, etc. need only be deployed where truly sensitive information is involved. For example, if only data labelled 'public' is being accessed, then integrity control is the only issue that need to addressed - confidentiality would no longer be a concern.

Labels alone are not sufficient to ensure the security of information. The security policy that applies to the information needs to be enforced by each organisation that handles it. All the organisations and individuals and their IT systems that process an item of data are presumed to know the relevant security policy. Organisations that exchange information need to establish trust in one another, to be satisfied that information will be handled according to agreed security policies. This trust is usually established through a formal agreement. Such security policies and agreements are outside the scope of this requirement.

An important aspect of security labels is that their integrity, and the integrity of their binding to the data, must be assured if the security policy is to be enforced.

A number of different bodies define security policies and their associated labels. Organisations define their own security policies for local communications within the organisation, and use private security labels. Groups of organisations each adopt a common security policy and use the security labels defined by the group, perhaps in conjunction with their own private security labels. There is also scope for a set of public security labels to permit secure communications between organisations world-wide.

Annex C. Business Scenarios

In healthcare, clinical and regulatory requirements are leading to needs for systems that can provide more granular access control across the increasing volume of patient data. The ability to mark (label) various data elements as guidance to an access control system is essential to meet these requirements. Proprietary systems currently exist to provide this functionality, but the pressure would have to increase significantly over existing requirements to force a departure from more open solutions.

Information relating to safety-critical systems must be clearly labelled as requiring special handling.

In the entertainment industry, the ready distribution of material via the Internet, for example, has led to the need for labelling to allow systems to be set up to screen out automatically material according to the classification of its content by violence, sex, language, etc.

Many Governments have comprehensive schemes for marking data for confidentiality. Proprietary systems incorporating labels do exist, but without a clear standard for labelling, it will remain difficult and expensive to interconnect systems securely, both within a Government and with other organisations.