INTRODUCTION

Enterprises are increasingly dependent on the use of IT systems to support their business operations by the delegation of responsibility for the management and control of the information on which their businesses are based to those IT systems. As the technology of IT systems improves then the architectures of the IT systems themselves are changing to reflect the actual organisation and operations of the enterprises they support. The IT system resources are becoming distributed throughout an enterprise and the demands for inter-operability between, and the interconnectivity of, IT systems both within and between enterprises is increasing.

In order to survive an enterprise is responsible for the safe custody and maintenance of its assets. These assets comprise both tangible and intangible assets. The greatest intangible asset is generally the information on which the enterprise manages its business, in fact its business may be the provision of information.

The responsibility for the protection of the assets of an enterprise rests with the board of directors, or equivalent body or individual, who are therefore the ultimate security authority for the enterprise. The security policy for an enterprise identifies the security relevant assets of the enterprise, who is responsible for them, and how they should be accessed and managed. The scope of applicability of the security policy is the management domain of the security authority.

The board of directors may delegate to heads of departments the authority and responsibility for enforcing the specific aspects of the enterprise security policy that apply to the assets under the control of the department. When those assets are information held on IT systems, then aspects of security policy are further delegated to the IT systems themselves. The departments and IT system can themselves be considered as security domains enforcing a security policy specific to the activities and assets within their own domains. Such security domains are subdomains of the overall enterprise domain.

In order for an IT system to take responsibility for enforcing aspects of the enterprise security policy, the information, policy rules and procedures of the enterprise security policy must be translated or mapped to IT system elements, rules and activities.

A simplified example is illustrated in Figure 1. Within the enterprise security domain, the policy states that only the owner of a document is permitted to view it or modify its contents. Each individual has an attribute, his or her name; each document has an attribute, its owner. Within the IT system domain, processes represent users; files represent documents. Each system element is assigned an attribute corresponding to that of the entity it represents in the enterprise domain. Thus, the process attribute identifies the user; the file attribute identifies the owner. The policy rule is mapped to controlling read and write access by the process to the file, and permits access if and only if the process attribute equals the file attribute.

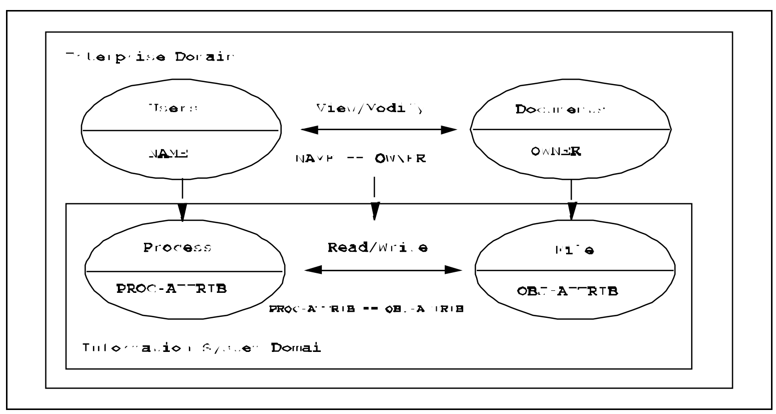

Figure 1 Example of IT System as Subdomain of Enterprise Domain

The operations of an enterprise involve interactions between security domains, both between its own subdomains and between its own security domain and the security domains of other enterprises. Similarly, an IT system may be decomposed into a set of security subdomains and its operations modelled as a set of interactions between security domains both between its own subdomains and with other IT system security domains.

The purpose of this security framework is to support the modelling of such a decomposition and to identify the security services, and thence the APIs, necessary to support the enforcement of security within an IT system.

SECURITY CONCEPTS

The security concepts introduced above are now more formally described based upon the ISO definitions.

Security Policy

A security policy is a set of rules that constrain one or more sets of security-relevant activities of one or more sets of elements. A security policy need not apply to all activities or all elements in a distributed system. This means that instances of its use must include a definition to which activities and to which elements the security policy applies. [ISO 10181-1]

A security policy must include a definition of the scope of the security domain to which it applies. In particular, a security policy may be specific to a particular service within an IT system.

Security Authority

A security authority:

- is responsible for the implementation of a security policy (which may be null in some cases);

- may be a composite entity; such an entity must be identifiable and responsibility rests with it and not its components;

- may, depending on any security policy that the security authority may be subject to, delegate the enforcement of the security policy to one or more entities;

- may, depending on any security policy the security authority may be subject to, delegate responsibility over some or all of its activities and some or all of its elements within its security domain to one or more entities.

Two security authorities are said to be linked if they are constrained to coordinate their security policies. [ISO 10181-1]

Within an IT system the security authority is represented by the security services supported by the system. The activities of the security services are controlled by the security information configured by the security authority of the enterprise domain of which the IT system is a subdomain. That is, authority within an IT system is derived, by delegation, from the security authority of the enterprise the IT system is managed by. In addition a security authority is typically represented by more than one entity within an IT system, for example an operating system together with a set of security relevant applications each of which is responsible for some aspect of the overall security policy and/or some subset of the elements and activities of the IT system.

Security Domain

A security domain is a set of elements under a given security policy administered by a single security authority for some specific security relevant activities. The activities of a security domain involve one or more elements from that domain, however at least one of the elements must be in that domain. [ISO 10181-1]

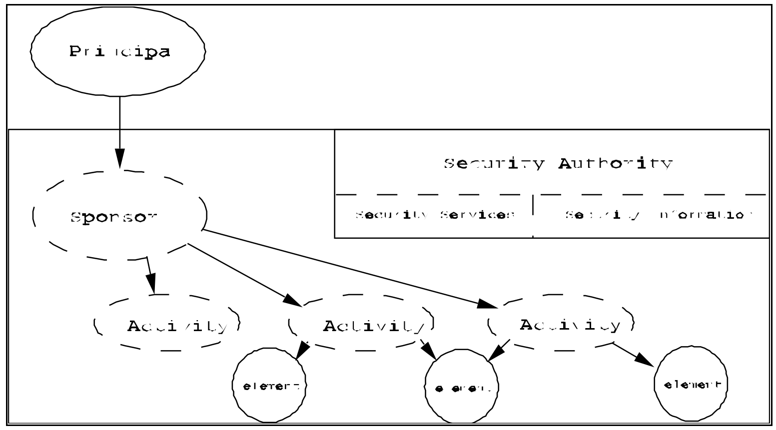

Figure 2 Security Domain

Within this framework a security domain provides services to principals which are external to the domain. See figure 2. A principal may be an end-user, ie., an individual, or a service within another security domain acting on behalf of an end-user or service. Principals are required to interact only with a sponsor located within the security domain. The sponsor promotes[1] the principal within the security domain both facilitating and constraining the principal's interactions with the activities and elements of the domain. The sponsor is responsible for the enforcement of the domain security policy through the invocation of the domain security services.

The security authority is represented within the security domain by a set of security information together with a set of security services which utilise the security information maintained by the security domain to enforce the security policy. The security information is associated with the elements and activities of the domain and with elements and services external to the security domain such as principals or external security authorities with which an inter-relationship exists or an interaction has been established.

A subset of the services supported by the security domain will be management services for the maintenance of the security information on which the security services are based.

The generic threats to the elements and activities of a security domain, as detailed in ECMA TR/46, can be summarised as :

unauthorised disclosure of information
unauthorised modification of information
unauthorized use of resources
misuse of resources
unauthorized information flow
repudiation of information flow
denial of service

and the methods of attack as:

access by unidentified or misidentified principals (cannot be trusted to fulfil responsibilities under policy)

introduction of unauthorized resources in addition to or in substitution

---

[1] The combination of a sponsor and the promoted principal can be considered to map to the concept of security subject in terms of which security policies are typically expressed.

of authorised resources (cannot be trusted to enforce policy)

misuse of management facilities (enforcement of policy depends upon integrity and completeness of security information)

traffic analysis (inference of information flow by analysis of information flow both within or into/out of a security domain.

In general a security domain is required to:

- protect the integrity, and maybe confidentiality, of its elements and activities,
- ensure the availability of, and account for the use of, the elements and activities under its protection.

To meet the generic requirements identified above the sponsor and the domain security services must:

- verify the principal's authorization to use the domain's services, requiring authentication of the principal's identity or security information presented as proof of authorization,
- mediate the principal's access to the activities and elements of the security domain on the basis of the access rights associated with the principal within the security domain. This will include mediation of access to the security services and security information representing the security authority of the domain,
- record a principal's use of the security domains services and access to the security domains elements to provide accountability for their use.
- protect the integrity and confidentiality of the activities and elements of the domain including providing for the segregation of the domain's elements and activities from any other domain's activities and elements.

It is a responsibility of a security policy of a security domain to identify the specific threats and detail the specific security measures to be taken to address those threats within that security domain.

A security domain does not necessarily provide all the security measures detailed above but may place reliance upon security domains comprising its environment to provide some of the protective measures required. A security policy is required to specify assertions on the security relevant behaviour of the environment of the security domain necessary to ensure the successful enforcement of the security policy within the domain.

This will include assertions on the responsibilities of principals authorised to use the security domain services, eg., not to disclose passwords, and especially upon those principals with administrative responsibilities over the security domain.

INTERACTIONS AND INTER-RELATIONSHIPS BETWEEN SECURITY DOMAINS

The operations of enterprises and IT systems depend upon interactions between security domains. In order for interactions to take place between security domains, it is necessary that there be common aspects in the security policies of the domains. This is termed the secure interaction policy.

A secure interaction policy defines which subset of elements of each associating security domain comprise the common security domain and the set of permitted activities.

A secure interaction policy is established by the exchange of security information between the security domains. This occurs within two contexts, an administrative context and an operational context.

- Administrative Context

  In the administrative context the exchange of security information is persistent. It defines the elements, permitted activities and the policy which must operate between the associating security domains. An example is the exchange and installation of security information pertaining to the authentication of principals, this may be cryptographic keys, passwords, or address of an authentication service.

  If the associating security domains are independent security domains then negotiation will be required between the security authorities of the associating security domains.

  If the associating security domains are both subdomains of a common superdomain then the secure interaction policy may be defined, and the associated security information established, by the security authority of the common superdomain.

- Operational Context

  In the operational context the exchange of security information is transient and related to the formation of an instance of an association to service a particular set of transactions between the associating security domains. The interaction will occur within the context of secure interaction policy and the security information exchanged will be, or will be derived from, that established previously by the administrative action creating or maintaining the common security domain.

PLATFORM AND SERVICE DOMAINS

A particular distinction can be made between two types of security domain within an IT system[2]; service domains which provide information processing services to principals in the context of enterprise operations (applications), and platform domains which control and structure the physical and processing resources of an IT system into elements that may be used by the service domains (infrastructure).

Platform domains structure the physical resources of an IT system, processor memory, data storage and communication media into identifiable elements with assigned security characteristics and mediates the flow of data between these elements. In order to successfully enforce the policy of data flow mediation the services of a platform domain are presented at a protected, non-bypassable interface. That is a platform domain fulfils the role of a Reference Monitor in the TCSEC definition. A platform domain is typically substantiated by operating systems communication systems. The actual interfaces and services presented by a platform domain are dependent upon the implementation. They may be represented by an interface equivalent to POSIX.1 system service interface, such as traditional UNIX kernel implementation, or by a microkernel interface with POSIX.1 system services implemented as service domains.

---

[2] The terminology used, platform and service domains, is an attempt to address confusing in the use of the terms application and infrastructure. Any better suggestions are welcome. See appendix on terminology.

Service domains are substantiated by the elements of platform domains, eg., processes, files, and communication channels. Thus inter and intra service domain operations involving interactions and data flow between platform domain entities are subject to the security policy enforced by the platform domains.

The inter-relationship between service domain components and a platform domain is that of subdomain to superdomain. The platform domain enforces a basic policy on the activities of the service domain but may delegate some aspects of policy enforcement to a particular service domain component assigned that responsibility, ie., a process which possesses a particular capability[3].

TRUST

Element x trusts element y for some classes of activity in the context of a security policy if and only if element x has confidence that element y will behave in a well-defined way that does not violate the security policy. [ISO 10181-1]

The administrative actions that establish a secure interaction policy between two security domains establish a trust relationship between them. Each trusts the other to behave in a manner that does not violate the secure interaction policy. The security information exchanged is evidence of the establishment of the trust relationship. An example of this form of relationship will be the exchange of information whose privacy is to be protected. Regardless of any security measures implemented within or over the communication services transferring the information the originator must trust the recipient to uphold the privacy security policy once the information is delivered into the recipient's custody.

Similarly a trust relationship exists between a subdomain and a superdomain and is established by the administrative actions on integrating the components of an IT system into a whole. For example the assignment of security attributes, including capabilities, to service domain components, ie., program and data files.

Particular trust dependencies arise between a service domain and the platform domains which substantiate it in order to maintain the integrity of the security services of the service domain. These are, derived from ECMA-138:

- Protect the security services and objects against external corruption. That is provide protection for the elements substantiating the service domain against unauthorised access by elements not constituting part of the service domain. For example, privacy of process address space.

- Provide the OSI communications security services (for example peer entity authentication) requested when forming associations, or indicate that it is unable to do so.

- Provide the necessary initial security information to security services and objects. For example, cryptographic master keys and identities for service domains.

- Enforce use of an appropriate authorization service for each access request. That is the mediation of access to platform entities cannot be bypassed.

- Direct all initial human user contact to a subject sponsor and secure this link according to the local security policy. This is the requirement for a trusted path. Within this framework this

[3] Previously referred to as privilege.

requirement extends to any initial contact by a principal must be directed to a component acting as sponsor for a security domain.

APPENDIX - TERMINOLOGY

This is included as a discussion point.

Application

- Within the POSIX and X/Open environments the term application refers to any caller of the system or other service APIs. This does not imply any concept of the service provided by the application nor of the security awareness of the application.

- The common use of the term application by end-users is to a software package providing a specific set of functionality, eg., a wordprocessor. Such functionality is end-user orientated and will depend upon the provision of other services, such as printing and file storage, perceived as system services by the end-user.

- Within the ISO OSI model the term application is a more generic term referring to an entity providing any service that is represented at layer 7 in the OSI model. More specifically, an application comprises a set of one or more application service elements.

Infrastructure and Operating System

The terms infrastructure and operating system have several interpretations:

- The POSIX and X/Open specifications refer to system service and communication service APIs which provide access by processes to the physical and processing resources of the system. These services are provided by the operating system and communication services.

- The ISO security framework does not make any reference to operating systems or infrastructure. However, the OSI model distinguishes between; the lower layers (1 to 4) which are considered to handle data and provide end-system to end-system interconnection, and the upper layers (5 to 7) which handle information and provide application entity to application entity interconnection.

- ECMA uses the term infrastructure to refer to the operating systems and communication services supporting applications.

- End-users and application developers typically consider an operating system to comprise the operating system together with commands, utilities, and system services. That is, the operating system services together with a set of applications.

- System integrators will consider some applications to comprise part of the system infrastructure when they provide services used by other applications, eg., printing, email, and database services.

APPENDIX - COMMON SYSTEM CONFIGURATION

This is included as a placeholder to describe the different configurations and the changes in threats between them. It may be better included after a discussion of security information and the need to protect and propogate it.

Standalone System

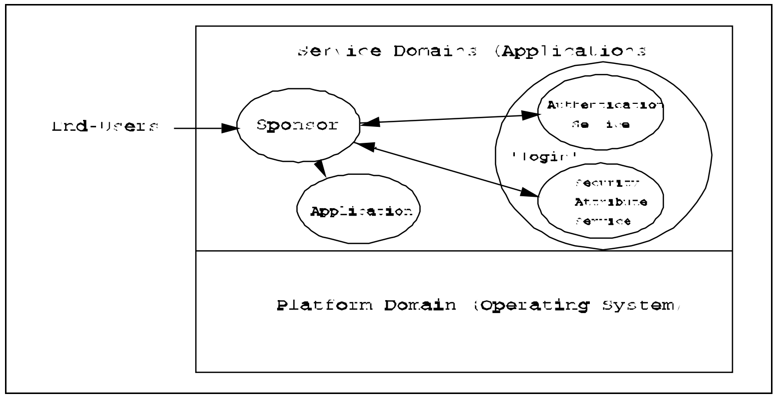

Figure 3 Standalone System

A standalone system comprises a single platform domain which supports a set of applications, or service domains as illustrated in Figure 3. The platform domain and its applications are under the control of a single administrative authority. This authority establishes the trust relationships within the system by configuring security attributes on software installation. Specific capabilities, for example, may be assigned to an application. The attributes on the elements of the platform, ie., on its processes, files, intercommunications channels, may be pre-set, or are set using trusted utilities, viz., applications.

The platform domain then enforces security policy with respect to those elements, and the security attributes assigned to them. All applications trust the platform domain to maintain the association of the principal's security attributes with the chain of processes which are executed on the principal's behalf. In addition, the platform provides services allowing applications to interrogate those attributes as required. The platform maintains the segregation of service domains, their data resources; it maintains the integrity and confidentiality of their contents.

Interconnected Systems

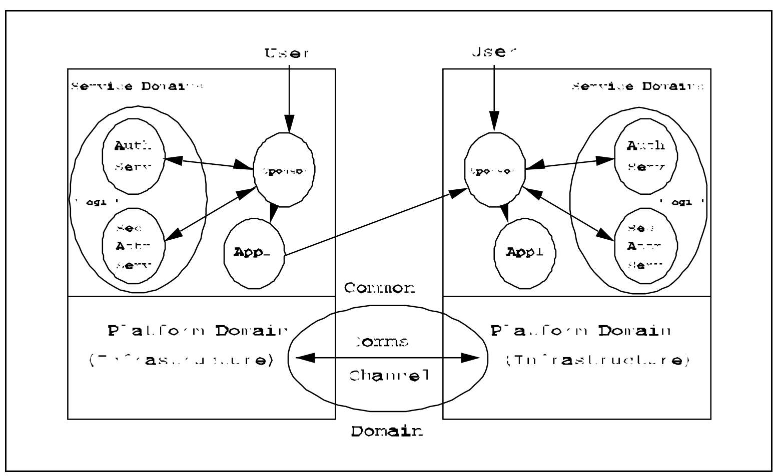

Figure 4 Interconnected Systems

When two systems are connected as illustrated in Figure 4, each system remains responsible for its own security services. An interconnection policy needs to be established, defining how, and when the systems can communicate, and the nature of those interactions. Each system then needs to be configured such that the security information they contain supports the formation of operational inter-relationships between the two systems. A communications channel provides the means by which elements in one system may be accessible to the other.

Each system remains responsible for the authentication of users of its respective services. Hence, a principal is required to authenticate itself separately to each system it wishes to use. This involves providing a set of security information meaningful to the system accessed.

The communications channel needs to protect the data transmitted through it. Thus, it must provide segregation of data resources and protection of the integrity and confidentiality of their contents. This can rarely be achieved by solely physical means and often cryptography is used to provide the basic protection required.

Distributed Systems

A distributed system is a set of interconnected systems which place a mutual trust in certain security services which may be shared between systems, such as authentication and security attribute services. In order to do so, security information needs to be propagated throughout the distributed system in a reliable way. In a standalone system, the platform is trusted to maintain the association of security attributes with a chain of process execution. In a distributed system, the association of security attributes is more complex: the security information needs to be propagated in such a way that the attributes are protected from threats within the communications system and ensures their authenticity and integrity.

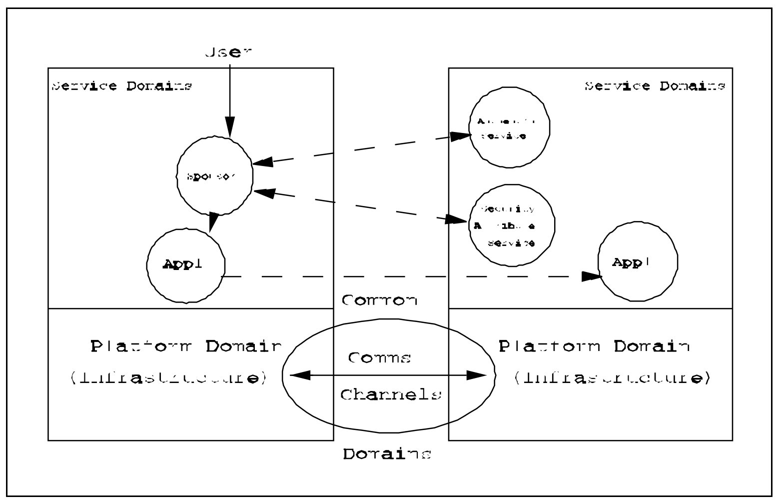

Figure 5 Distributed System