Section 3: Security Concepts

3.1 Introduction

Enterprises are increasingly dependent on the use of Information Technology (IT) systems to support their business operations. As the technology of IT systems improves, 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 interoperability between, and the interconnectivity of, IT systems both within and between enterprises is increasing.

An enterprise is responsible for the safe custody and maintenance of the information on which the enterprise relies to manage and conduct 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, aspects of security policy are further delegated to the IT systems themselves. The departments and IT system can 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. The enterprise domain is a superdomain of the subdomains.

This is illustrated in Figure xxx. Authority is delegated to four depatments. Departments C and D further delegate authority to IT systems under their control. Departments A and B both delegate authority over some of their information and activities to the same IT department, which in turn delegates authority to an IT system.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

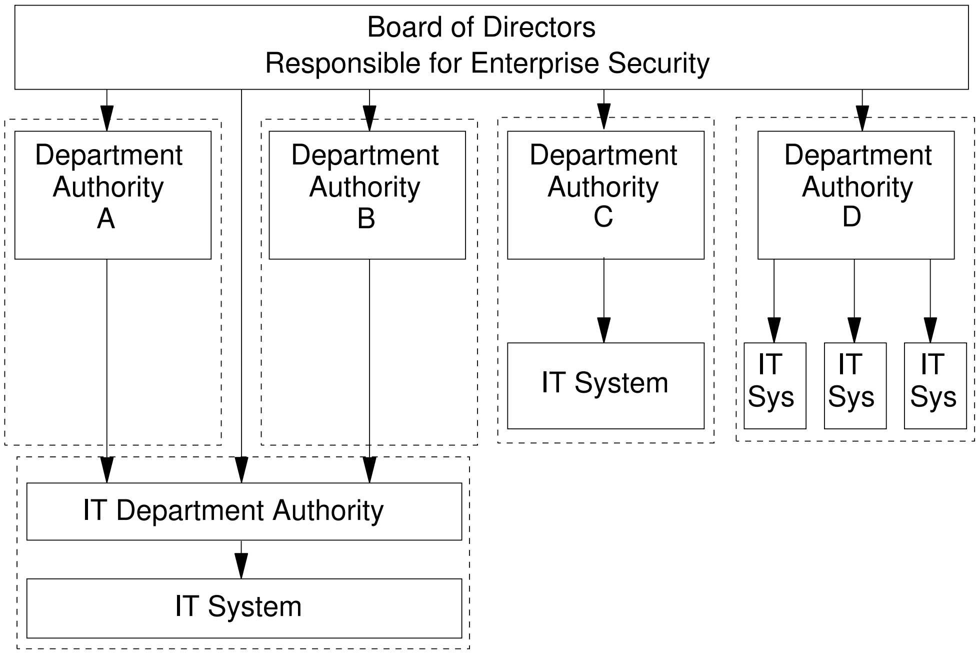

Figure 3-1 – Delegation of Authority within an Enterprise Domain

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.

One of the purposes of this security framework is to support the modelling of such a decomposition and to identify the security services, and from them the APIs, necessary to support the enforcement of security within an IT system.

A simplified example is illustrated in Figure xxx. 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: a 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 regulates read and write access by the process to the file, and permits access if and only if the process attribute equals the file attribute.

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

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

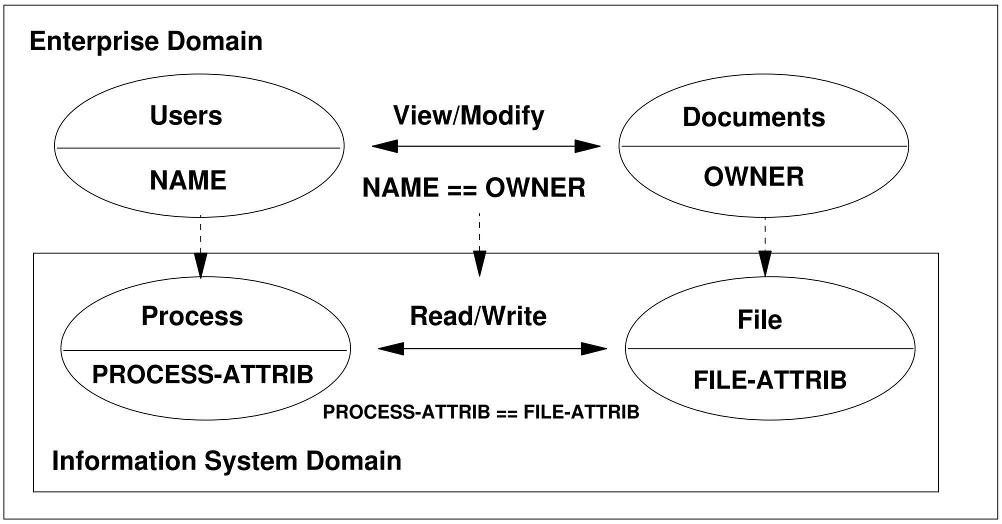

Figure 3-2 – The IT System as a Subdomain of the Enterprise Domain.

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 security concepts introduced above are more formally described in the following sections based upon the definitions in the ISO Security Framework [ISO 10181-1].

NOTE: *ISO reference needs to be built in using cross reference macros. See page 39 of Style Guide.*

3.2 Security Policy

A security policy is a set of rules that constrain one or more sets of security-relevant activities and 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 of the activities and the elements to which the security policy applies.

Within an IT system the activities are the processing operations and the elements are the data stored and processed.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

3.3 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 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. For example, two security authorities need to coordinate any changes to the allocation of user identities exchanged between their systems when interworking.

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 which manages the IT system. In addition a security authority is typically represented by more than one entity within an IT system. For example a security authority can be an operating system together with a set of security relevant applications each of which is responsible for some aspect of the overall security policy or some subset of the elements and activities of the IT system.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

3.4 Security Domain

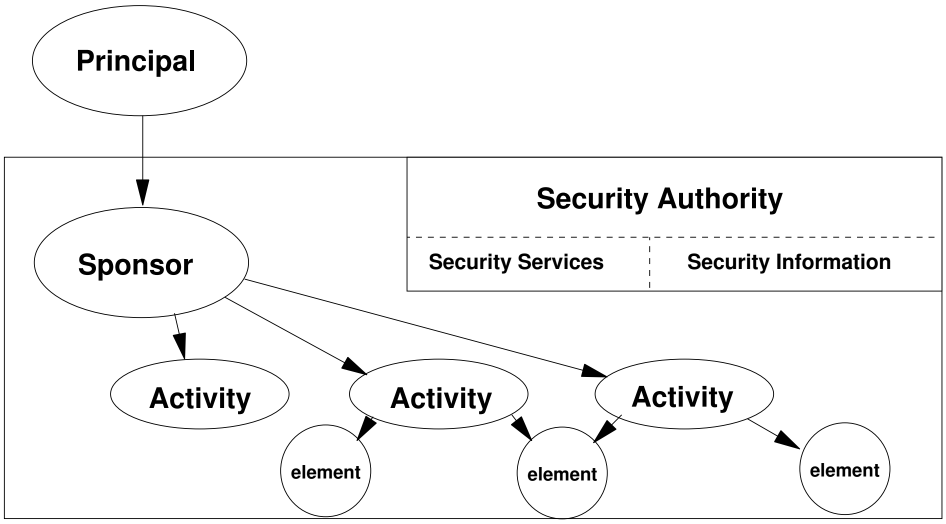

Figure 3-3 – Security Domains

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.

Within this framework a security domain provides services to principals that are external to the domain. See Figure xxx. A domain service is provided by the invocation of all, or a subset, of the domain activites on all, or a subset, of the domain elements. A principal may be an individual or a service within another security domain acting on behalf of a individual or another service. Principals are required to interact only with a sponsor located within the security domain. The sponsor promotes 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 direct and indirect 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 that utilise the security information maintained by the security domain to enforce the security policy. The

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

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 are management services for the maintenance of the security information. Security management services and security information are also activities and elements of the security domain.

At the highest level the security objectives defined by a security policy for a security domain are generally to:

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

It is a responsibility of the security policy of a security domain to identify the specific threats to the integrity, confidentiality, and availability of the activities and elements of that domain and detail the security measures to be taken to address those threats within that security domain.

3.5 Generic Threats

From the perspective of users and owners, the threats to information and information processing systems are usually categorised under the following main headings:

- Unauthorised Modification
- Unauthorised Disclosure
- Unauthorised Use of Resources
- Denial of Service
- Repudiation.

Even at this level of definition it is impossible clearly to separate each area of threat. The realisation of a threat in one area often increases the risks of other types of threat occurring.

3.5.1 Unauthorised Modification

This covers the unauthorised modification of information and information processing resources and services that can prejudice the business of nations, organisations and individuals.

The concern here is the maintenance of the integrity of information. The threats are to the procedures and processes involved in ensuring that business-sensitive

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

and critical information is introduced, changed and removed in an authorised manner. Examples are the modification of information relating to: sales and purchase orders, funds transfer, electronic mail and military signals, with the intention of defrauding or confusing.

The realisations of this threat may include the unauthorised modification of the software and hardware base of the information system, which may then accidentally or intentionally facilitate the realisation of other threats.

3.5.2 Unauthorised Disclosure

This covers the unauthorised disclosure of information that may damage the interests of a nation, organisation, or individual.

Concerns over the confidentiality and privacy of information vary. At one end there are government and defence concerns over the disclosure of national and alliance classified information. For most enterprises the need is to protect business confidential information. From the point of view of individuals the primary need is for privacy. This last need is variously addressed in data privacy legislation and similar obligations on the holders of personal data.

NOTE: Certain classes of system management and configuration information, especially that which is security relevant, constitutes sensitive information that should not be disclosed without authority.

3.5.3 Unauthorised Use of Resources

The unauthorised use of system resources includes the theft of hardware and software components, as well as the unauthorised use of information systems and the services they provide.

Apart from physical theft, the most common concern here is masquerade, the unauthorised *impersonation* of an authorised user or other entity by discovering and using his authentication credentials.

The threat of masquerade is not limited to users; malfeasant systems and services may attempt to impersonate authorised systems and services.

The unauthorised use of information system resources and services may result in embarrassment and cost penalties to the owners, as well as leading to unauthorised disclosure, modification, and denial of service.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

3.5.4 Denial of Service

Denial of service covers actions and events that prevent information processing systems from providing agreed levels of service to authorised users.

Denial of service threats range from the environmental acts of nature and man, such as fire, flood and bombs, to more targeted threats, for example the accidental or intentional swamping of an electronic mail service with a large volume of unwanted messages.

The results of different types of denial of service threats can range from catastrophic loss through to no more than a temporary suspension of a service. But even the latter could have a significant impact on the business of an enterprise. For example, consider the impact in the stocks and shares market of the suspension, for a few active trading hours, of some part of an organisation's IT based trading services.

3.5.5 Repudiation

This covers the subsequent denial by an initiator or a target of having performed some business-sensitive or security-sensitive information processing operation.

This category of threat covers many forms of denial of accountability or responsibility. It includes the denial that a message was sent or received by the sender or receiver. Where such messages are being relied on for the conduct of business or some other endeavour, then such a denial may damage the interests of one or both parties involved.

3.6 Generic Countermeasures

To meet the generic security requirements and address the generic threats identified above, the sponsor and the domain security services may use the following countermeasures:

- verify the principal's authorisation to use the domain's activities, requiring authentication of the principal's identity or of security information presented as proof of identity or authorisation,

- 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 includes mediation of access to the activities and elements that form the security services and security information representing the security authority of the domain,

- record a principal's use of the security domain's services and access to the security domain's elements to provide accountability for their use.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

• 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.

3.7 Interactions and Interrelationships between Security Domains

The security relevant operations of enterprises and IT systems generally require interactions between security domains. These interactions take the form of activities that cross domain boundaries and elements that are shared by the domains. To establish security management and control of these interactions it is necessary to formulate a secure interaction policy.

A secure interaction policy defines which subset of the elements of each associating security domain comprise the common security domain and defines 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 that 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 is 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.

NOTE: Note that it is possible to establish a unilateral policy, for example anonymous ftp, in which no administrative exchange actually occurs. However, administrative action is required in the target domain.

In this case the concept of a secure interaction policy still applies, however, no security information is required to be exchanged. The access control policy in the target domain permits access to the system by any principal but constrains the activities and elements that can be accessed.

Operational Context

In the operational context the exchange of security information is transient and occurs during the formation of an instance of an association to service a

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

particular set of transactions between the associating security domains. The interaction occurs within the context of a secure interaction policy and the security information exchanged is, or is derived from, that established previously by the administrative action creating or maintaining the common security domain.

3.8 Assertions on Domain Environment

A security domain's environment include's its parent or superdomain, subdomains to which it delegates authority, and other domains with which it interacts. A security domain does not necessarily provide all the security measures detailed in xxx above but may rely upon other security domains comprising its environment to provide some of the protective measures required. The security policy of a security domain is required to specify assertions on the security relevant behaviour of the security domain's environment necessary to ensure the successful enforcement of the security policy within the domain. Hence other security domains that comprise the environment must satisfy these assertions.

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

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.