Information Systems Security

ISSN: 1065-898X (Print) 1934-869X (Online) Journal homepage: https://www.tandfonline.com/loi/uiss19

Security Functional Components for Building a Secure Network Computing Environment

Manpreet Singh UCOE & Manjeet Singh Patterh UCOE

To cite this article: Manpreet Singh UCOE & Manjeet Singh Patterh UCOE (2007) Security Functional Components for Building a Secure Network Computing Environment, Information Systems Security, 16:6, 332-343, DOI: 10.1080/10658980701747245

To link to this article: https://doi.org/10.1080/10658980701747245

Published online: 19 Dec 2007.

Information Systems Security, 16:332–343, 2007

ISSN: 1065-898X print/1934-869X online
DOI: 10.1080/10658980701747245

Taylor & Francis
Taylor & Francis Group

Security Functional Components for Building a Secure Network Computing Environment

Manpreet Singh and Manjeet Singh Patterh
UCOE, Punjabi University, Patiala, India

ABSTRACT It is difficult to define reliable security policy components that should be applied to validate a secure computing environment. The job gets further complicated when one has to deal with multiple policies in single computing environment. This paper demonstrates how we can overcome the difficulties of defining reliable security components by using evaluation criteria. In this paper we use common criteria to derive the security functional components for a multipolicy-based network computing environment. In the verification process, the derived policy components are related to the specific security objectives of the network communication environment. The evidence listed in the case study supports the claims that the proposed network security policy interpretation framework is a complete and cohesive set of requirements.

1. INTRODUCTION

The success in achieving a high degree of security in a network system depends on the degree of care that is put into designing a security model. The work on modeling security in stand-alone computer systems has attained a degree of maturity (Bell & LaPadula, 1973; Biba, 1977; Salzer & Schroeder, 1975; Gasser, 1988; Landwehr, 1981, Goguen & Meseguer, 1982; Mclean, 1990; Sandhu, 1994), but in the context of network systems few security models exist that address all dimension of the security problem of network system operating environment. More work is still needed, particularly in defining an appropriate and reliable security model for a network system and its environment that addresses the network security problem comprehensively.

The security model design requires clear understanding of the security functional requirements (FIP Standard, 2004; FIP Standard, 2006; NIS Special Publication, 2002; NIS Bulletin, 2003). In the literature we found various approaches being used by researchers to investigate access control security requirement. The two main approaches being used by researchers for establishing security requirements are the threat analysis-based approach

Address correspondence to Manpreet Singh, UCOE, Punjabi University, Patiala, India.
E-mail: mspattar@gmail.com

and the evaluation criteria-based approach. Threat analysis is essential and has been studied intensively by reseachers (Debar et al., 2006; Thomson & von Solms, 1998; von Solms, 1996; von Solms et al., 1994; White, Fisch, & Pooch, 1996; Whitman, 2004). However, as evaluation processes for computing environment security evolved and computing technologies progressed, the standard evaluation criteria-based approach gained in popularity among researchers. The most general framework in the area of computing environment security has been carried out by the U.S. Department of Defense and the European Union, resulting in standard evaluation criteria now popularly known as the Common Criteria (ISO/IEC, 20050. This should be the basis for every attempt to model security of the computing environment and where we focus in this paper. The newness and the lack of experiences in the exercise of the Common Criteria make it imperative that efforts be exerted to investigate the prospective influence of the Common Criteria in advancing the state of security.

This article aims to provide basis for specifying security functional requirements through interpretation of standard computer system security functional components defined in the Common Criteria. We begin our development process with the identification of the relevant security functional components in the standard system evaluation criteria (Department of Defense, 1985; Department of Trade & Industry, 1991; NIS, 1992; ISO/IEC, 2005; Common Criteria, 2006), which can serve as basis for the design of the framework. After the identification of the suitable security functional components, an interpretation is formulated that extends the identified components to meet the security functional requirements of the network system and its operating environment reliably. The derived interpretation is used to design the policy oriented network security functional framework.

The remainder of the article is organized as follows: Section 2 describes the evaluation criteria considerations for trusted system environment. Section 3 describes policy-oriented security functional components. Section 4 provides the interpretation of security functional components for network systems. Network policy validation with real world case study is presented in section 5, and section 6 presents the conclusions of this work.

2. SYSTEM SECURITY EVALUATION CRITERIA AND COMPONENTS

To formally evaluate a system, the credible body of experts requires a standard evaluation methodology. The evaluation methodology provides a set of requirements defining the security functionality for the system. Several evaluation standards have affected formal evaluation methodologies. Major standards include the Trusted Computer System Evaluation Criteria (TCSEC), the Information Technology Security Evaluation Criteria (ITSEC), and the Federal Criteria (FC). These standards remained centered on operating systems and were found inadequate to evaluate the new emerging products and network-based systems. To address the inadequacies in the above standard, the major foundational methodologies have culminated in the Common Criteria, which today has worldwide support. In this paper our aim is to use standard evaluation methodology as guidelines to precisely determine the appropriate security functional requirements for network systems.

Security Functional Components in Standard Evaluation Criteria

The Trusted Computer System Evaluation Criteria, also known as the Orange book, was the first major computer security standard evaluation methodology developed by the U.S. government. The TCSEC is organized by evaluation class, and each evaluation class contains security requirements. These security requirements are presented in TCSEC in the context of computer security evaluation methodology and are identified as Discretionary access control requirements, Objects reuse requirements, Mandatory access control requirements, Label requirements, Identification and Authentication requirements, and Consistent Informal/Formal Security Policy Model.

The above requirements are represented in TCSEC under six evaluation classes C1, C2, B1, B2, B3, and A1, as shown in Table 1.

The ITSEC took a different approach to evaluation than that of the TCSEC, and consequently it successfully addressed some of the shortcomings of the TCSEC. In ITSEC a product or system that is the subject of evaluation is termed as a target of

TABLE 1 **TCSEC evaluation class**

Evaluation Class	Name	Security Requirements
C1	Discretionary protection	1.DAC 2. .I&A
C2	Controlled access protection	1.DAC 2.I&A 3.OR&A
B1	Labeled security protection	1.MAC 2.LR 3.SPM (Informal)
B2	Structured protection	1.MAC 2.LR 3.SPM (Formal)
B3	Security domain	1.Audit Requirements 2.B2 (Requirements)
A1	Verified design	1.B3 (Requirements) 2.Stringent Audit Reqs.

evaluation (TOE). The ITSEC provided 10 classes of security functionality, labeled from F1 to F10. These classes were listed from lowest to highest. Each class included the requirements of the preceding level. The mapping between ITSEC security functionalities classes and TCSEC security classes is shown in Table 2.

The development of Federal Criteria (FC) was another effort to address the shortcomings of the TCSEC and ITSEC. The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) together developed the FC. Technically, the FC was heavily influenced by the TCSEC but followed the lead of the ITSEC in its separation of assurance and functional requirements. The product or system evaluation in the FC is done with respect to protection profiles. A protection profile is an abstract specification of the security aspects of a product or system and is product independent. The FC also introduced the concept of a product dependent security target that implemented the requirements of an approved protection profile.

The TCSEC, ITSEC, and FC provided the necessary foundations for the next de facto security evaluation standard named Common Criteria (CC), which today has worldwide support. The CC support two kinds of evaluations: Protection Profiles (PP) and products or systems against security targets (ST).

The requirements expressed in PP or in a ST are termed as Security Functional Requirements (SFRs). The SFRs describe the desired security behavior expected of a Target of Evaluation (TOE). The SFRs include multiple Security Function Policies (SFPs). Each SFP has a scope of control that defines the subjects, objects, resources or information, and operations controlled under the SFP. All SFPs are implemented by the TOE Security Functionality (TSF), whose mechanisms enforce the rules defined in the SFRs and provide necessary capabilities.

TABLE 2 **Mapping between ITSEC functionality classes and TCSEC security classes**

ITSEC Security Functionality	TCSEC Security Classes
F1	C1
F2	C2
F3	B1
F4	B2
F5	B3
F6	A1

For user data protection in standalone system environments, CC defines two major families of SFPs: Access Control SFPs and Information Flow Control SFPs. Access control SFPs base their policy decisions on attributes of the users, resources, subjects, and objects. These attributes are used in the set of rules that govern operations that subjects may perform on objects. Information Flow Control SFPs base their policy decisions on the attributes of the subjects and information within the scope of control and the set of rules that govern the operations by subjects on information. The attributes of the information may be associated with the attributes of the container or may be derived from the data in the container. The attributes stay with the information as it is processed by the TOE Security Functionality.

The rules that define the functionality of the access control and information flow control SFPs will be defined in the Access control functions (DP_ACF) and Information flow control functions (DP_IFF) families, respectively. Based on the identified elements of SFRs related to the SFP, appropriate security functional component should be selected. Below is the description of the security functional components supported by TOE to provide user data protection.

3. POLICY-ORIENTED SECURITY FUNCTIONAL COMPONENTS

Access Control Policy Components and Functions (DP_ACC)

Access Control Policies Components (ACC)

The access control policy components are used to represent access control SFPs and define the scope of control of the policies that form the identified access control portion of the SFRs related to the SFP. The scope of control is characterized by three sets: the subjects under control of the policy, the objects under control of the policy, and the operations among controlled subjects and controlled objects that are covered by the policy, that is, the access control SFP covers a set of triplets: subject, object, and operations.

The access control policy components are capable of representing the access control SFPs to be enforced by the traditional Discretionary Access Control (DAC) mechanisms. The access control components (ACC) are identified as follows (see Table 3):

- Subset access control (SA_ACC)
- Complete access control. (CA_ACC)

Access Control Policy Functions

Access control functions describe the rules that can implement an access control policy identified in Access control policy (DP_ACC), which also specifies the scope of control of the policy. The access control functions are identified as follows.

- Security attribute based access control functions. (SA_ACF).

Security attribute-based access control provides requirements for a mechanism that mediates access control based on security attributes associated with subjects and objects. Each object and subject has a set of associated attributes, such as identity, time, location, owner, or group.

The access control security functions can also be used to explicitly authorize or deny access to an object based upon security attributes. This functionality could be used to provide privilege, access rights, or access authorizations within the TOE. Such privileges, rights, or authorizations could apply to users, subjects, and objects.

TABLE 3 Access control components

	Subset Access Control-Level 1	Complete Access Control-Level 2
Access control	Access control on subset of operation	Access control on all operation

Information Flow Control Policy Components and Functions (DP_IFC)

Information Flow Control Policies Components (IFC)

The information flow control policy components are used to represent information flow control SFPs and define the scope of control of the policies that form the identified information flow control portion of the SFRs related to the SFP. The scope of control is characterized by three sets: the subjects under control of the policy, the information under control of the policy, and operations that cause controlled information to flow to and from controlled subjects covered by the policy, that is, information flow control SFP covers a set of triplets: subject, information, and operations that cause information to flow to and from subjects.

The information flow control policy components are capable of identifying the information flow control SFPs to be enforced by the traditional Mandatory Access Control mechanisms. The TSF mechanism used to enforce information flow control SFRs controls the flow of information in accordance with the information flow control SFP.

The information flow control components are identified as follows (Table 4).

TABLE 4 Information flow control components

	Subset Information Flow Control -Level 1	Complete Information Flow Control-Level 2
Information flow control	Information flow control on subset of operation	Information flow control on all operation

- Subset information flow control (SIF_IFC)
- Complete information flow control (CIF_IFC)

Information Flow Control Policy Function (IFF)

Information flow control functions describes the rules that can implement the information flow control SFPs named in Information flow control policy (FDP_IFC), which also specifies the scope of control of the policy. The information flow control functions are identified as follows.

- Simple Security attributes based information flow control function(SSA_IFF)
- Hierarchical Security attributes based information flow control function.(HAS_IFF)

Simple Security attributes based information flow control function requires security attributes on information, and on subjects that cause that information to flow and subjects that act as recipients of that information. The attributes of the containers of the information should also be considered if it is desired that they should play a part in information flow control decisions or if they are covered by an access control policy.

Hierarchical Security attributes based information flow control function requires the use of hierarchical security attributes that form a lattice, that is, information flow between a controlled subject and controlled information via a controlled operation is based on the ordering relationships between security attributes. To enforce hierarchical Security attributes based information flow control functions, the information flow control security attributes should support the following relationships.

- There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable;
- There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
- There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

The above information flow control security functions can also be used to explicitly authorize or deny an information flow based upon security attributes. This functionality could be used to implement a privilege policy that covers exceptions to the basic policy defined within TOE.

In the next section we use the security functional components introduced in this section as a basis to derive security function component interpretation for network system and its operating environment.

4. INTERPRETATION OF SECURITY FUNCTIONAL COMPONENTS FOR THE NETWORK SYSTEM

The approach of using standalone security functional components as a basis for interpretation has the advantage, as with a trusted standalone system, of a network system that also has to manage shared resources and mediate access to those resources by the subjects under its control, in accordance with a security functional policy. In the proposed interpretation for network system:

- All SFPs can be termed as network security functional policies (NSFPs) and are associated with network entities instead of with network system.
- To specify entity level security functional policies, appropriate security functional component supported by network entities has to be selected based on the identified portion of the network SFRs related to the NSFP.
- The NSFPs are implemented by the TOE Security Functionality (TSF) where TOE is a network system. The network as a whole possesses a single TSF that can be referred to as NTSF, consisting of the totality of security relevant portions of the network.
- The NTSF provides the mechanism to enforce the rules defined in the network SFRs over the resources and information that the network system controls.

TABLE 5 Security functional component interpretation

Component Class	Security Functional Component	Network Interpretation
Network Access Control Policy Components	SA_ACC	SNA_ACC
	CA_ACC	CNA_ACC
Network Information Flow Control Policy Component	SIF_IFC	SNIF_IFC
	CIF_IFC	CNIF_IFC

- The NTSF is distributed over the network entities and is referred to as partitioned. At the level of network entity it is the NTSF partition that is responsible for the complete and correct enforcement of the elements of the overall network SFRs relevant to the network entity.
- The security functional components and functions supported by network entities are interpreted as per Table 5.

In the following, the network interpretation components given in Table 5 are discussed.

Network Access Control Policy Component and Functions (NDP_ACC)

Network Access Control Policies Components (NACC)

The network access control policy components are used to represent network access control SFPs and define the scope of control of the policies that form the identified access control portion of the Network SFRs related to the NSFP. The scope of control is characterized by three sets: the network subjects under control of the policy, the network objects under control of the policy, and the network operations among controlled subjects and controlled objects that are covered by the policy, that is, the network access control SFP covers a set of triplets: network subject, network object, and network operations. The network access control policy components are capable of representing the network access control SFPs to be enforced by the traditional Discretionary Access Control (DAC) mechanisms.

The network access control components (NACC) are identified as follows:

- Subset network access control (SNA_ACC)
  - Connection Control (CC)
  - Bind Control (BC)
- Complete network access control. (CNA_ACC)
  - Connection Control (CC)
  - Bind Control (BC)

Subset network access control requires that each identified network access control SFP be in place for a subset of the possible network operations on a subset of the network objects in the TOE. In this case the role of the network TSF is to enforce the network access control SFP on list of network subjects, network objects and network operations among network subjects and network objects covered by the network SFP.

Complete network access control, requires that each identified network access control SFP cover all network operations on network subjects and network objects covered by that network SFP. It further requires that all network objects and network operations protected by the network TSF are covered by at least one identified network access control SFP. In this case the role of the network TSF is to enforce the network access control SFP on list of network subjects and network objects and all network operations among network subjects and network objects covered by the network SFP.

Network Access Control Policy Function

Network access control functions describe the rules that can implement an network access control policy identified in Network Access control policy (NDP_ACC) which also specifies the scope of control of the policy. The network access control functions are identified as follows.

- Security attribute based network access control functions. (SA_NACF).

Security attribute based network access control provides requirements for a mechanism that mediates network access control based on security attributes associated with network subjects and network objects. Each network subject and network object has a set of associated attributes, such as user identity or group membership, user role, access rights,

network address, port address, communication protocol, domain name, time of the day or location.

The network access control security functions can also be used to explicitly authorize or deny access to a network object based upon security attributes. This functionality could be used to provide privilege, access rights, or access authorizations within the TOE. Such privileges, rights, or authorizations could apply to users, network subjects and network objects.

Security attribute-based network access control functionality may be specified using variety of mechanism like access control lists and capabilities. These mechanisms implement controls on subject and objects. Access control lists bind the data controlling access to the objects. Capability lists bind that data to the subjects. By careful drafting of the attribute based access control rules various organizations of these mechanisms can be used that lead to powerful controls.

Network Information Flow Control Policy Components and Functions (NDP_IFC)

Network Information Flow Control Policies Components (NIFCC

The Network Information flow control policy components are used to represent network information flow control SFPs and define the scope of control of the policies that form the identified network information flow control portion of the network SFRs related to the NSFP. The scope of control is characterized by three sets: the network subjects under control of the policy, the information under control of the policy, and network operations which cause controlled information to flow to and from controlled network subjects covered by the policy, that is, network information flow control SFP covers a set of triplets: network subject, information, and network operations that cause information to flow to and from network subjects.

The network information flow control policy components are capable of identifying the network information flow control SFPs to be enforced by the traditional Mandatory Access Control mechanisms. The network TSF mechanism used to enforce network information flow control SFRs controls the flow of information in accordance with the network information flow control SFP. Operations that would change the security attributes of information are not generally permitted as this would be in violation of a network information flow control SFP. However, such operations may be permitted as exceptions to the network information flow control SFP if explicitly specified.

The network information flow control components are identified as follows:

- Subset network information flow control (SNIF_IFC)
  - Information Flow Control (IFC)
  - Connection Control (CC)
- Complete network information flow control (CNIF_IFC)
  - Information Flow Control (IFC)
  - Connection Control (CC)

Subset network information flow control requires that each identified network information flow control SFPs be in place for a subset of the possible network operations on a subset of information flows in the network system. In this case the network TSF shall enforce the information flow control SFP on list of network subjects, information, and network operations that cause controlled information to flow to and from controlled network subjects covered by the network SFP.

Complete network information flow control, requires that each identified network information flow control SFP cover all network operations on network subjects and information covered by that SFP. It further requires that all network information flows and network operations controlled by the network TSF are covered by at least one identified network information flow control SFP. In this case the role of the network TSF is to enforce the network information flow control SFP on list of network subjects and information and all network operations that cause that information to flow to and from network subjects covered by the SFP.

Network Information Flow Control Policy Function (NIFF)

Network Information flow control functions describes the rules that can implement the network

information flow control SFPs named in Network Information flow control policy (NDP_IFC), which also specifies the scope of control of the policy. The network information flow control functions are identified as follows:

- Simple Security attributes based network information flow control function (SSA_NIFF)
- Hierarchical Security attributes based network information flow control function (HSA_NIFF)

Simple Security attributes based network information flow control function requires security attributes on information, and on network subjects that cause that information to flow and network subjects that act as recipients of that information. The attributes of the containers of the information should also be considered if it is desired that they should play a part in network information flow control decisions or if they are covered by a network access control policy.

Hierarchical Security attributes based network information flow control function requires the use of hierarchical security attributes that form a lattice, that is, information flow between a controlled network subject and controlled information via a controlled network operation is based on the ordering relationships between security attributes. To enforce hierarchical Security attributes based network information flow control functions, the information flow control security attributes should support the following relationships.

- There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable;
- There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
- There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

The above network information flow control security functions can also be used to explicitly authorize or deny an information flow based upon security attributes. This functionality could be used to implement a privilege policy that covers exceptions to the basic policy defined within network system.

In next section we consider a case study to validate how well the interpreted security functional components described in this section maps to the security functional requirements of an organization.

5. SECURITY POLICY FRAMEWORK VALIDATION: A CASE STUDY

In this section we consider a case study of an organization with following security objectives.

Security Objectives

The security objectives of the enterprise network system are stated as follows.

O.IA

The network system must identify a user uniquely and ensure that only authorized users gain access to the network system and its resources.

O.INTEGRITY

The network system must protect the reliable data from the unauthorized disclosure, modification, and deletion. The Reliable data Security Functional policies (RD_SFP) for an organization are as follows.

- *RD1.SFP*: Data related to company future plans is to be kept secret from competitors.
- *RD2.SFP*: Customer personal data and information as provided by customer to company as a part of purchase are to be available only to those who process the order.
- *RD3.SFP*: Release of sensitive data requires the consent of the company's official and lawyers.
- *RD4.SFP*: Organizations that are part of extranet like suppliers of raw material and distributor are

to be given access to that part of information, which is required by them to perform business transaction with organization.

O.ACCESS_CONTROL

The network system must enforce the access to network resources on the basis of the identity of the network entities.

O.INFO_FLOW_CONTROL

The network system must enforce access to resources on the basis of the access level of the network subjects and network objects.

O.ACCESS_LEVEL

The network system must assign and revoke the access level of the network subjects and the network objects according to the organization access control policies.

O.MANAGE

The network system must provide all the function and facilities necessary to support administrative users who are responsible for the management of the network system security and must ensure that only administrative users are able to access such functionality.

Security Policy Assumption

A.NSO

Network Security Officer (NSO) is the only user in the entire enterprise who can assign the access classes to network subject and objects.

A.CRYPT

An appropriate cryptographic protocol and cryptosystems exists for the protection of the information transmitted over an enterprise network.

A.IA

A highly reliable network-based authentication mechanism is provided for user's identification.

A.PHYSICAL_SEC

Physical security measures exist to protect network devices and communication links for reliable transfer of information across the network.

A.ACCESS_CLASS

All entities within the enterprise network have comparable access classes and unique identification.

A.TRUSTED ADMINISTRATOR

Authorized administrators of Enterprise network system are not ill-willed users, and educated with network system management functions, and perform their duties appropriately according to administrator's guidelines.

Organization Policy

The organization policy of enterprise network system is stated as follows.

P.IA

Only those users who have been authorized to access the information within the network system may access the system.

P.INFO_FLOW_CONTROL

The right to access specified network objects at particular access level is determined on the basis of the access level of the network subject.

P.ACCESS_CONTROL

The right to access specific network object is determined on the basis of the identity of the network subject.

NETWORK SYSTEM SECURITY FUNCTINAL REQUIREMENTS.				
CLASS	COMPONENT		FUNCTION	
Network Access Control	NACC.1	NACP_Connection Control (NACP_CC)	SA_NACF.1	NACP_Connection Control Function
	NACC.2	NACP_Bind Control (NACP_BC)	SA_NACF.2	NACP_Bind Control Function
Network information flow control	NIFCC.1	NIFCP_Information Flow Control (NIFCP_IFC)	SSA_NIFF.1 HSA_NIFF.2	NIFCP_Information Flow Control Function
	NIFCC.2	NIFCP_Connection Control (NIFCP_CC)	SSA_NIFF.1 HSA_NIFF.2	NIFCP_Connection Control Function

FIGURE 1 **Network System Security Functional Requirements**

P.ACCESS_LEVEL

The network system must assign and revoke the access level of the network subjects and the network objects according to the organization access control policies.

P.ADMINISTRATOR

An authorized network administrator must manage the enterprise network system.

Network System Security Functional Components

Network system security functional components are specified in Figure 1.

SECURITY POLICY ENFORCEMENT AND VALIDATION

In this section we present the evidence used in network security policy validation. This evidence supports the claims that the proposed network security policy interpretation framework is a complete and cohesive set of requirements.

Network Security Objective Rationale

Figure 2 shows how the network security objectives map to the security functional policies defined for the network system.

Network Security Objectives / ASSUMPTIONS & NETWORK SECURITUY POLICIES	Network System Security Objectives					
	O.IA	O.MANAGE	O.INTEGRITY	O.ACCESS_CONTROL	O.INFO_FLOW_CONTROL	O.ACCESS_LEVEL
P.ACCESS_CONTROL			X	X		
P.INFO_FLOW_CONTROL					X	X
P.ACCESS_LEVEL					X	X
P.ADMINISTRATOR		X				
P.IA	X		X			
A.NSO		X				
A.CRYPT		X				
A.IA	X					
A.PHYSICAL_SEC					X	
A.ACCESS_CLASS					X	X
A.TRUSTED ADMINISTRATOR		X				

FIGURE 2 **Mapping Network Security Objectives to Assumptions and Policies**

O.IA

Since the network system must identify a user uniquely and ensure that only authorized users gain access to the network system and its resources, O.IA is required to counter P.IA with assumption A.IA.

O.MANAGE

Since the network system provides the means of managing securely by the administrative users, O.MANAGE is required to support P.ADMINISTRATOR with assumption A.NSO, A.CRYPT, and A.TRUSTED ADMINISTRATOR.

O.INTEGRITY

Since the network system must protect the reliable data from the unauthorized disclosure, modification, and deletion, O.INTEGRITY is required to counter P.ACCESS_CONTROL, P.INFO_FLOW_CONTROL and P.IA with assumption A.IA.

O.ACCESS_CONTROL

Since the network system must enforce the access to network resources on the basis of the identity of user, group, or network subject, O.ACCESS_CONTROL is required to counter P.ACCESS_CONTROL.

Network Security Objectives / Network Security Functional Components	Network System Security Objectives					
	O.IA	O.MANAGE	O.INTEGRITY	O.ACCESS_CONTROL	O.INFO_FLOW_CONTROL	O.ACCESS_LEVEL
NACC.1				X		
SA_NACF.1				X		
NACC.2			X	X		
SA_NACF.2			X	X		
NIFCC.1					X	
SSA_NIFF.1					X	
HSA_NIFF.2					X	
NIFCC.2					X	
SSA_NIFF.1					X	
HSA_NIFF.2					X	
A.IA	X		X	X	X	
A.TRUSTED ADMINISTRATOR		X				

FIGURE 3 **Mapping Network Security Objectives to Security Functional Components**

O.INFO_FLOW_CONTROL

Since the network system ensures the access to network resources on the basis of the security access class of network subject and network object, O.INFO_FLOW_CONTROL is required to counter policy P.INFO_FLOW_CONTROL and P.ACCESS_CLASS with assumption A.PHYSICAL_SEC.

O.ACCESS_CLASS

Since the network system must assign and revoke the security access level of the network subject and the network object according to the organization access control policies, O.ACCESS_CLASS is required to counter P.ACCESS_LEVEL and P.INFO_FLOW_CONTROL with assumption A.ACCESS_CLASS.

Network Security Policies Rationale

Figure 3 shows how the network security functional components map to the security objectives defined for the network system.

NACC.1 access control

This component satisfies O.ACCESS_CONTROL because it ensures the enforcement of the connection control element of the network access control policy on all network subjects and network objects.

NACC.2 access control

This component satisfies O.ACCESS_CONTROL and O.INTEGRITY because it ensures the enforcement of the secrecy and integrity element of network access control policy on all network subjects.

NIFCC. information flow control

This component satisfies O.INFO_FLOW_CONTROL because it ensures the enforcement of network information flow control policy on all network subjects.

NIFCC.2 information flow control

This component satisfies O.INFO_FLOW_CONTROL because it ensures the enforcement of connection control element of network information flow control policy on all network subjects.

6. CONCLUSIONS AND FUTURE WORK

In this paper we have focused on the development of policy oriented network security framework for enterprise networks. The proposed framework is used to model security environment for the enterprise network system. The framework gives a precise policy on how access control and information flow control should be enforced in multidomain environment. In developing the framework, policy components are related to the specific security objectives of the network communication environment. Thus the framework provides a basis for the design of secure architecture and policy for an enterprise computer network system

In our future work we plan to use our present study as a basis for the development of formal security policy model for network system evaluation.

REFERENCES

Bell, D.E., & LaPadula, L. J. (1973). Secure Computer Systems: Mathematical Foundations. Mitre TR-2547, Vol. 1. Bedford, MA: Mitre Corporation, November.

Biba, K. J. (1977). Integrity Considerations for Secure Computer Systems. Mitre TR-3153. Bedford MA: Mitre Corporation.

Common Criteria for Information Technology Security Evaluation (CC) (2005). version 2.3, ISO/IEC 15408:2005, August.

Common Criteria for Information Technology Security Evaluation (CC). (2006). version 3.1 Revision 1, September.

Debar, H., Thomas, Y., Boulahia-Cuppens, N., & Cuppens, F. (2006). Using contextual security policies for threat response, Lecture Notes in Computer Science, 109-128.

Federal Information Processing Standard 199. (2004). Standards for Security Categorization of Federal Information and Information Systems, February.

Federal Information Processing Standard 200 (2006). Minimum Security Requirements for Federal Information and Information Systems, March.

Gasser, M. (1988). *Building a Secure Computer System*. New York: Van Nostrand Reinhold Co., Inc., pp. 57-72.

Goguen, J., & Meseguer, J. (1982). Security policies and security models, Proceedings of the 1982 IEEE Symposium on Security and Privacy, Oakland, CA: IEEE Computer Society Press, p.11.

Information Technology Security Evaluation Criteria (ITSEC). (1991). Department of Trade and Industry, London, June.

Landwehr, C. (1981). Formal models for computer security, *ACM Computing Surveys*, 13: 3, p. 247, September.

Mclean, J. (1990). The specification and modeling of computer security, *Computer,* 23(1):9-16, January.

National Institute of Standards and Technology Special Publication 800-47. (2002). Security Guide for Interconnecting Information Technology Systems, August.

National institute of Standards and Technology and the National Security Agency. (1992). Federal Criteria (FC) for Information Technology Security, Volumes I and II, version 1, December.

National Institute of Standards and Technology. (2003). Information Technology Laboratory (ITL) Bulletin: Secure Interconnections for Information Technology Systems, February.

Salzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems, Proc. IEEE, vol. 63. pp. 1278-1308. Available at http://www.ieee.org/web/publications/procieee/

Sandhu, R. S., & Samarati, P. (1994). Access control: Principles and practice, *IEEE Communication Magazine*, September: pp 40-48.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively, *Information Management & Computer Security*, 6: 167-73.

Trusted Computer System Evaluation Criteria (TCSEC). (1985). Department of Defense, 5200.28 – STD, December.

von Solms, R. (1996). Information security management: the second generation, *Computers & Security,* 15: No.4, pp. 281-288.

von Solms, R., van de Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation, *Information & Management,* 143-153.

White, G. B., Fisch, E. A., and Pooch, U. W. (1996). *Computer System and Network Security*. Boca Raton, FL: CRC Press.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, 24: 43-57.