濟州大學校 産業技術硏究所 論文集, 第7卷, 1號, pp.93~100, 1996. 6
Cheju National Univ. R.I.I.T. Jour., Vol.7, No.1, pp.93~100, 1996. 6

Design and Implementation of a Security Management System for Secured OSI Directory Services

Wang-Cheol Song* and Jang-Hyung Kim*

보안화된 OSI 디렉토리 서비스에 대한 보안 관리 시스템의 설계 및 구현

송 왕 철* · 김 장 형*

ABSTRACT

In this paper, we have designed and implemented a security management system, which is based on the CMISE services. This system provides two security-related System Management Functions(SMFs) to security management users such as notification of a security event alarm and an audit trail of a security related event. These SMFs are implemented using osimis-4.0, OSI Network Management platform. The target of this security management system is secure X.500 directory services based on the Authentication Framework specified in the recommendation X.509. The security system is implemented using OSISEC and its services are data confidentiality, data integrity and non-repudiation of origin. Based on the OSI network management framework, we implemented a manager system which administers the keys and provides CMISE services, and also some remote agent systems which provide services for the events concerning the security system, while also interacting with MIB. Access Control SMF is being implemented.

Key words : Directory service, Security management system, SMF, MIB

Ⅰ. INTRODUCTION

As computer networks grow large, network management is one of the essential issues in computer network research[1,2,3,4,5]. With the ever-increasing pervasiveness of computer networks, information accessible through or transported by networks, as well as network components and resources themselves, are

* 제주대학교 정보공학과
Dept. of Information Eng., Cheju Nat'l Univ.

often at risk[6]. Information and network security are thus becoming the focus of intense concern on the part of network user and operators. Techniques for implementing network security are being standardized and products have started appearing on the market. Network operation and network security both require management. In fact, besides network configuration, fault, performance, and accounting functions, network security is the fifth aspect that has been recognized explicitly by the Open Systems Interconnection(OSI) architecture as requiring management functions.

The goal of this research is to design and implement a security management system which can be applicable to large computer networks. Before implementing it in a large network, first we have developed an experimental security management system, which can be used for secure X.500 directory services using OSISEC.

This paper is structured as follows. In section 2 we present functions and structure of a security management system in this research. We specify services of the designed and implemented security management system in section 3. Section 4 discusses implementation and operation of the system. In section 5 we present the conclusions of this research.

II. SECURITY MANAGEMENT

The main objective of security management is to create, delete, activate, suspend, query, update or otherwise maintain the status of managed security objects through continuous gathering or distribution of information about ongoing security-relevant activities, using proper management services and protocols, such as CMIS and CMIP in OSI networks.

Security management system is concerned with generating, distributing, and storing encryption keys. Passwords and other authorization or access control information is maintained and distributed. Security management system is also concerned with monitoring and controlling access to computer networks and access to the network management information obtained from the network nodes. As logs are an important security tool, two SMFs(system management functions) such as recommendation X.736 *security alarm reporting function*, recommendation X.740 *security audit trail function* are implemented.

OSI security system specified in recommendation X.800 facilitates secure interworking of the OSI services and provides security services, such as data confidentiality, data integrity and non-repudiation of origin. Its security mechanisms are encipherment, integrity checks and digital signature verification, while its security facilities are public key cryptography and hash functions.

Structures of the security manager and the agent and the target system are mentioned in some detail. First a manager belongs to and has authority over the domain managed by the certificate authority(CA) as long as it has control of key administration and credential generation. In addition a manager can access a MIB within a remote agent by first establishing a cross-certification between CAs through a manager of that remote agent. All these processes map operations such as creating and invocating of CA, and issuing of certificate into MOs thus letting the security management system manager take on CA

manager role through management operation to an agent.

As shown in figure 1, an agent stands between a manager and MIB. It collect information from each managed objects and transfers this information to a manager. It also perform an action issued by a manager. A manager communicates with an agent using CMISE, while the agent maps security related events into MOs, stores logs on them, and performs notification operations to the manager.

operations, founded on *strong authentication* of the users identity;

+ The Directory Service must enable users to trust the information that they extract by allowing DUAs to check the *integrity* of the information supplied. This can be done either by *authenticating* trusted source DSAs or by storing *signed information* in the entries.

Secure QUIPU implements countermeasures to counter some threats taken from X.509 such as identity interception, masquerade, replay, data interception, manipulation and repudiation.

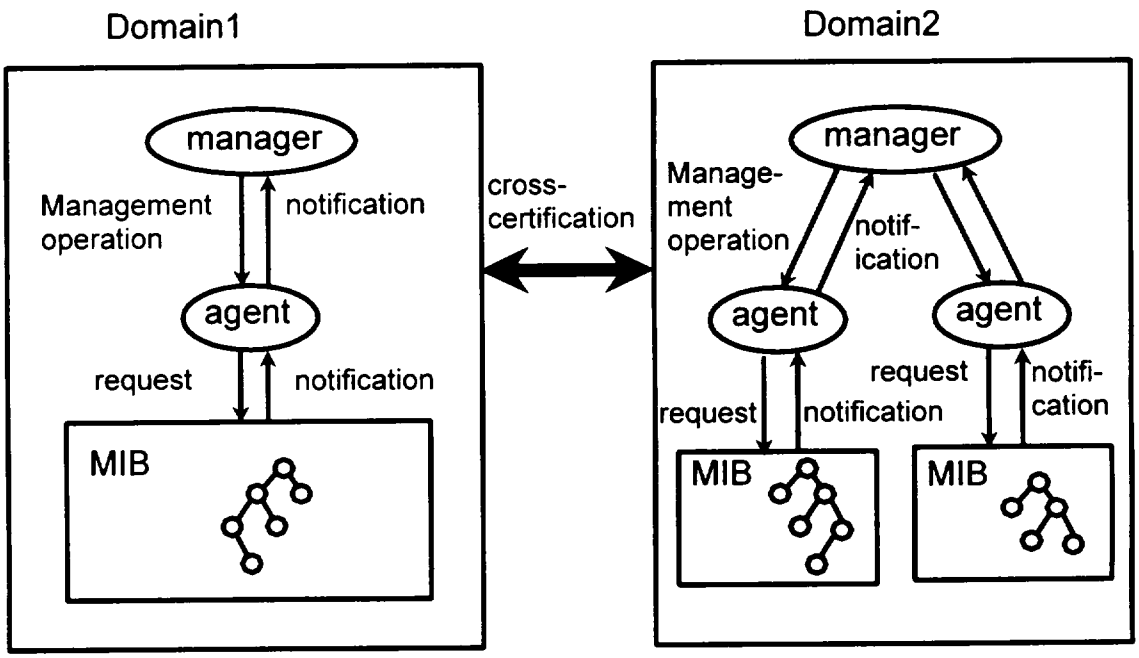

Figure 1. Conceptual model for security management systems

The target system for security management is secure X.500 directory services. It is implemented using secure QUIPU included in OSISEC. The fundamental security requirements for X.500 Directory Services are considered to be :

+ The enforcement of personal *access rights* for the read, search and modify

These threats address the user need for three security critical operations :

+ The simple *read* operation - requiring the user to provide a Distinguished Name to return information from the corresponding entry where attribute types and values are provided via the *read* operation, whereas validation of purported values is provided via

compare operation.

+ The *search* and *list* operation - enabling the user to derive from a fuzzy or simple specification of entry attributes the Distinguished Name(s) of entries found at different depths and search starting points in the DIT.

+ The *modify* operation - allowing the user to create and destroy master data entries, and to modify their attribute values.

Naming a managed object is one of important factors in a network management system. In the ISO management framework, it provides location transparency to the management systems.

The structure of a manager is presented in figure 2 and the functions of each elements is following :

Directory Service

One can get information about location of an agent using the directory service. The directory server maps the name of an agent in the form of AVA(attribute value assertion) into a network address. Also, this service was set as the target system in this research

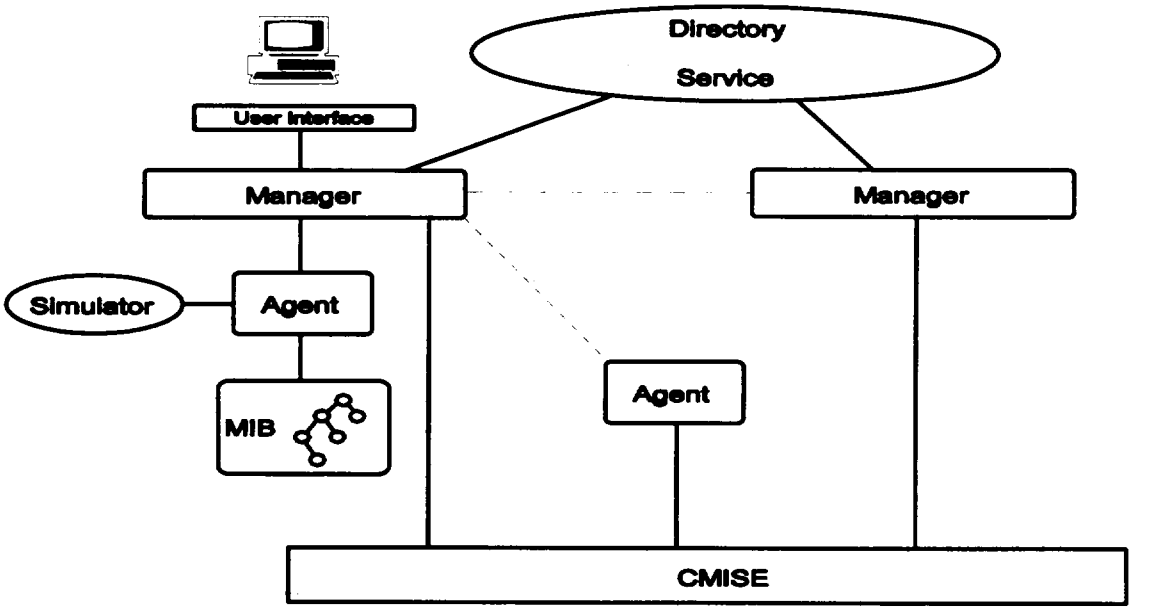

Figure 2. The structure of a security manager

the registration hierarchy scheme was introduced for identifying managed objects. The domain name system was introduced in the Internet[7]. After considering these, we chose the naming scheme which is equal to that of the OSI network management for compatibility. The directory server has name-to-address translating functions so that and enables the secure provision of network information to the users. It provides location transparency to the manager and at the same time stores the security related events such as MOs in the MIB.

CMISE

CMISE provides common management

facilities to management applications. With it, seven possible types of service primitives can exist as follows: M-EVENT-REPORT, M-GET, M-CANCEL-GET, M-SET, M-ACTION, and M-DELETE[8,9]. These are implemented as separate processes in osimis-4.0 and can be used as integrated form through GUI(graphic user interface).

Simulator

The simulator consists of two functions : security alarm reporting function(X.736) and security audit trail function(X.740). Security alarm reporting function models the reporting of security-related events and misoperation in security services and mechanisms and provides services for creating, deleting, and modifying event-forwarding discriminators for controlling the selection of security alarms and their distribution to manager specifiable destinations. Security audit trail function specifies the kinds of event reports that should be contained in a log that is to be used for evaluating the security of an open system. Security audit trails can be used to look for security attacks that are detectable as they occur.

Management Information Base(MIB)

MIB is one of the vital components to a network management system. Generally we can say that a MIB is a composite of management information about managed objects, that is, a set of managed objects and attributes.

Managed Object(MO)

This is a resource to be monitored and controlled by a network management system. We introduced an object-oriented design method in defining managed objects. A real resource can be characterized by four aspects. These are attributes, operations, notifications and behavior, which are concepts adopted from an object-oriented design technology.

User Graphic Interface

A user can interface with a security manager in a graphic display and can interactively input parameters of each service primitive. This interface is based on the X-window library system which offers the users management operations in an integrated environment.

III. SERVICES

In this paper, we implemented a security management system using osimis-4.0. This osimis-4.0 provides application programming interfaces(APIs) for the development of manager and agent applications in a generic fashion at different levels of complexity. At the lower level, an implementation of the OSI CMIS/P called the management Service Access Point(MSAP) is used to transfer information between managers and agents. MSAP makes use of the ISODE ACS, ROS and ASN.1 support services. At the higher level, object-oriented APIs in C++ are offered to the OSI application developer. Firstly, the agent API called Generic Managed System (GMS) hides aspects such as object addressing, scoping, filtering and error handling. GMS also hides most of the generic management functionality such as event reporting, event logging and access control.

Therefore, we make following services optimized for security management system using the user commands in osimis-4.0.

mibdump

mibdump enables a manager to connect to a remote OSI management agent and retrieve management information. A manager specifies the agent within the same domain and retrieves some informations from MIB. To access an Agent in another domain, the manager must be cross-certified.

mset

It is used to set MO attributes, and the '-w', '-a', '-r', '-d' options should be used to specify the attribute names and the corresponding values to be set. The difference is the set mode, which is the following for each option:

Option	Mode	Comments
-w	write	replace/set
-a	add value	for set-valued attributes
-r	remove value	for set-valued attributes
-d	default set	no value required

After each of these options, there should be an attribute value assertion of the form <attrType>=<attrValue>.

maction

It allows to perform a management action on MIBs. It treats key generation, key distribution and key revocation.

mcreate

It allows to create managed objects in MIBs. A manager must create *security* MOs for security related notifications, actions and logs

mdelete

It allows to delete managed objects from MIBs.

evsink

It requests and receives security-alarm report as well as event report from an MIB.

evlog

It allows a manager to use logging activities on an agent. It does this by allowing the creation and deletion of alarmRecord object, auditRecord object, and Log object, and by allowing certain attribute values of the alarmRecord and auditRecord object to be set, controlling its behaviour.

IV. Implementation and Operations ofSecurity Management System

In security management the most critical thing is key management. Because the cryptography participates a major role in the service and it is based on key generation, key distribution, and key storage, when a security system provides services such as strong authentication, confidentiality, integrity or non -repudiation. Additionally, in a multi-domain environment, a manager has to communicate with a manager in a remote domain. In constructing a multi-domain environment the most important thing is how access control and authentication are applied to each access.

This security management system is implemented using osimis-4.0 installed integrated with OSISEC. As the access control is provided by osimis-4.0, we are only concerned with the key management and security event alarm and audit trail. As the certificate authority (CA) in a security system is responsible for the key management and the certificate management, a management system manager in this system takes the role of the CA manager through the management system manager performing *maction*

management operation by abstracting CA's functions as MOs. Therefore, security services such as cross-certification is realized by the security system and this management system is managing the security services by methods that corresponding several functions to real resources of MOs. In addition, monitoring security system is implemented using the functions defined on ITU-T recommendations X.736 and X.740.

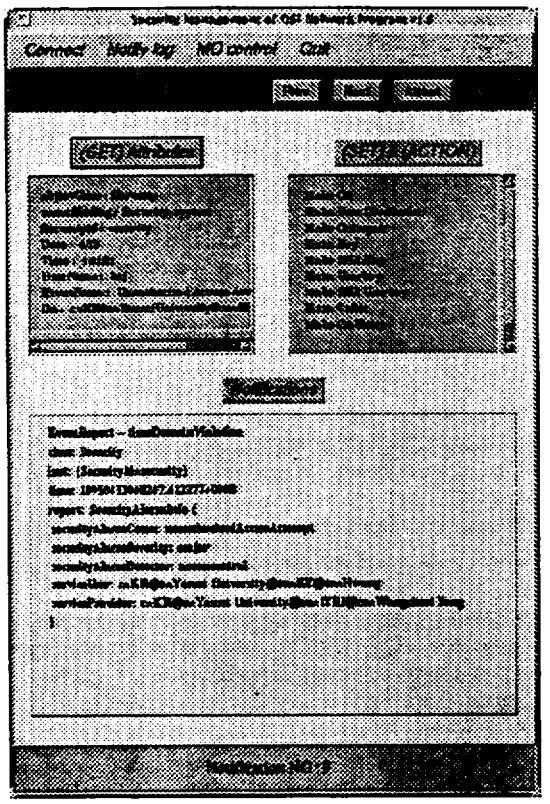

Figure. 3 User graphic interface

We made a User Graphic Interface that enables to input parameters of each service primitive interactively(fig 3). This interface is based on the X-window library system which offers the user management operations in an integrated environment.

IV. CONCLUSION

In this research the structure of a security management system is defined. This security management system, which is one of the management functional areas, is implemented. This is based on the OSI network management concept. Though we have implemented the management system in a LAN environment of our Lab., it can be extended to any type of network environment. We have introduced the management domain concept and object-oriented scheme for defining managed object and implementing manager and agent. The system implemented is the proto-type one at now, but the new version of our system is to be made.

V. 요 약

본 논문에서는 CMISE 서비스를 기초로 하는 보안관리 시스템을 설계 및 구현하였다. 이 시스템은 두가지 보안 관련 시스템 관리 기능들(SMF)를 구현하였는데 이들은 각각 보안 사건 알람의 통보와 보안관련 사건의 감시추적 기능을 수행한다. 이 기능들은 osimis-4.0을 이용하여 OSI 망관리 플랫폼하에서 구현되었다. 보안관리 시스템의 대상은 X.509에 근거한 보안화된 디렉토리 서비스이다. 이 관리 대상인 보안 시스템은 OSISEC을 이용해 구현되었고 데이터 기밀성, 무결성과 데이터 발송자의 부인 봉쇄 기능을 제공하고 있다. 본 보안관리 시스템은 OSI 망관리 시스템의 개념에 입각하여 구현되므로써 관리자는 키 관리 및 CMISE 서비스들을 제공할수 있게 하고, 원격 대행자들은 보안 시스템과 관련된 사건들에 대해 관리 서비스를 제공함은 물론 MIB와 상호작용하게 하였다.

REFERENCE

1. Ben-Artz, et al., "Network Management

of TCP/IP Network: Present and Future", IEEE Networks, Vol. 4, No. 4, July 1990.
2. A. Leinwand and K. Fang, Network Management: A Practical Perspective, Addison-Wesley, 1993
3. L. N. Cassel, et al., "Unified Network Management Architecture and Protocols: Problems and Approaches", IEEE SAC, Vol. 7, No. 7, Sep. 1989.
4. F.Halsall and N. Modiri, "An Implementation of an OSI Network Management", IEEE, Network, Vol. 4, No. 4, July 1990.
5. C. A. Sunshine, et al., "A Platform for Heterogeneous Interconnection Network Management", IEEE, SAC, Vol. 8, No. 1, Jan. 1990
6. Neumann P. G., "Illustrative risks to the public in the use of computer systems and related technology", ACM softw. Eng. Newsletter, Vol. 16, No. 1, 1991.
7. M. T. Rose, The Simple Book : An Introduction to Management of TCP/IP-Based Internet, Prentice-Hall, 1991.
8. ISO/IEC 9595, Common Management Information Service Definition, May 1990.
9. ISO/IEC 9596, Common Management Information Protocol Specification, May 1990.
10. Wangcheol Song, Lee-Hyun Baek and Chang-Eon Kang, "Design and Implementation of a Security Management System," IEEE SICON/ICIE'95, July, 1995.