초고속 정보통신망 시스템에서 보안 기술 설계

장승주**, 윤재우*, 김성관**

*한국전자통신연구원, **동의대학교 컴퓨터공학과

Design Security Features of High Speed Network

Jang Seung-Ju**, Yoon Jae-Woo*, Kim Sung-Kwan**

ETRI, Dongeui Univ., Dept. of Computer Engineering

요 약

초고속 통신망 시스템에서 CNM(Customer Netw ork Management) 시스템은 네트워크 시스템에 대한 자원 관리 및 정보 관리의 책임을 맡는 시스템이다. 이 시스템에 대한 보호는 네트워크 관리보다 훨씬 중요하다. CNM 시스템에 대한 외부 불순 세력의 접근은 전체 시스템의 파괴를 의미한다. 본 논문은 초고속 통신망 시스템에서 CNM 시스템에 대한 보안 기능 및 요구사항에 대한 설계 내용을 중심으로 언급한다. 보안 기능을 만족하기 위한 CNM 시스템 내의 기능으로 IDS 의 설치와 방화벽의 설치를 들 수 있다.

1. 서론

초고속 통신망 시스템에서 CNM 시스템 (Customer Network Management System, 이하 CNM 시스템) 은 고객망 관리 서비스를 제공하기 위하여 가입자측의 CNM 응용 (application) 과 대응되어 망 사업자내부에 위치하여 각 가입자 망의 관리 정보 제공과 실시간 장애경보 통지 및 가상연결에 관한 제어 의뢰를 받아 이를 수행하는 시스템이다. 이외에도 CNM 시스템은 광의의 관점에서 고객의 서비스 요구와 문제 관리에 관한 부분적인 기능, 즉, 문제 관리 (trouble administration) 에 관한 인터페이스 기능이나 서비스 오더의 부분적인 변경 및 특정 가입자 그룹에 대한 모니터링 전용 인터페이스 제공과 같은 기능들을 제공한다. CNM 시스템은 다음과 같은 역할을 수행하여야 한다.

- 가입자 인증
- 가입자가 사용하고 있는 ATM, Frame Relay 가상 연결의 상태, 대역폭, QoS, 연결 식별자 등의 구성 정보 제공
- 가입자단 UNI 구간의 A TM / FrameRelay / IP 레벨의 상태, 트래픽, Port type, 구성된 가상 연결의 수 등에 관한 관리 정보 제공
- 가입자단 UNI 구간의 자원 구성정보의 변경
- 단대단 ATM, Frame Relay 가상 연결의 생성, 제거, 변경
- 단대단 가상 연결로 이루어진 ATM / Frame Relay 가상 사설망의 관리 정보 조회, 제어
- 고객 망 관리 정보에 관한 보고서 제공 기능
- ATM, Frame Relay, IP 레벨의 망 서비스 사용에 관한 trouble ticket 을 접수받아 문제 해결을 도모할 수 있도록 문제관리를 위한 인터페이스 제공
- 운용자의 개입없이 가입자 정보 및 서비스 계약에 관한 정보를 변경, 조회할 수 있는 기능

이러한 CNM 시스템은 불순한 세력에 의한 보안 문제가 발생할 소지를 안고 있다. CNM 시스템에 발생하는 보안 문제는 이 시스템의 통제를 받는 네트워크 전체에 영향을 미치게 된다.

본 논문은 초고속 통신망 시스템내 CNM 시스템에 필요한 보안 요구사항에 대한 설계를 중심으로 언급한다. 2 장에서는 보안 요구사항, 3 장은 보안 시스템 설계 내용, 4 장 결론의 순으로 언급한다.

2. 보안 요구 사항

초고속 통신망 내의 CNM 시스템에 필요한 보안의 목적은 다음과 같이 정의할 수 있다.

- confidentiality
- Data 무결성
- 행위에 대한 책임소재 확인
- 가용성

보안 위협 요소는 다음과 같이 정의할 수 있다.

- 사칭(masquerading, spoofing)
- eavesdropping
- unauthorized access
- loss or corruption of information
- repudiation

- forgery
- denial of service

CNM 시스템에 필요한 기능적인 보안 요구사항은 다음과 같이 정리할 수 있다.

[표 1] 기능적인 보안 사항

기능	설명
Verification of ID	- M4 I/F 는 이런 기능을 지원 - 인증 기능이 M4 I/F 기능과 맞물려 동작
Controlled Access and Authorization	- 인증이 되지 않은 사용자에 대한 자원이나 정보에 대한 접근 차단 기능을 M4 I/F 가 갖는다
Protection of Confidentiality	- 저장된 데이터나 교환되는 데이터에 대한 안전성을 M4 I/F 는 보장
Protection of Data Integrity	- 사용자와 관련된 정보의 보호 - 다른 보안 서비스에서 사용되는 서비스에 대한 보호
Activity logging	- 관리 기능에 대한 행적을 추적할 수 있도록 함
Audit	- log 된 데이터에 대한 분석 및 추적 작업이 가능
Functional Classes for Security	- minimal functional class - basic functional class - advanced functional class

2.1 요구사항

CNM 시스템에 대한 보안 요구 사항은 ATM Security Service Management, 일반적인 요구사항으로 나눌 수 있다.

2.1.1 ATM 보안 서비스 관리

CNM 시스템의 ATM 망에서의 보안 관리 기능중 ATM 보안 서비스 관리에 대한 요구사항을 정리하면 아래의 표와 같다.

[표 2] ATM 보안 서비스 요구 사항

기능	설명
관리 기능	- entity authentication service - data confidentiality service - data origin authentication and integrity service access control service
Entity 인증	- 노드간에 보안 통신을 설정하는데 사용 - 인증을 할것인지 말것인지의 결정은 VC by VC 로 이루어짐
Data confidentiality	- 두 노드간에 정의 - 데이터 기밀성은 ATM 네트워크의 각 노드에 관심을 둬야함
data origin 인증 및 무결성	- ATM user 의 endpoint 에 초점
Access control	- 보안 메시지 교환 및 형상 파라메타 정보에 대해서 행해짐 - 관리는 각 노드에 대해서 행해짐 - control panel 에 대한 경우는 두 노드 간에 이루어짐

2.1.1 ATM 보안 서비스에 대한 형상 관리

CNM 시스템에서 ATM 보안 서비스에 대한 형상관리 정보를 표로 정리하면 다음과 같다.

[표 3] ATM 보안 서비스 형상 관리 요구 사항

기능	설명
기본적인 연산	- create, modify, read, activate, deactivate, delete
형상 관리	- operation 상태 - administrative 상태
Operational 상태	- resource 를 실제 설치 및 작동시킬 것인지에 관한 연산 - operational resource 는 operation 상태 특성으로 반영 - disabled/enabled 로 구분(resource 상태를 enable 또는 disable 상태로 조정 가능)
Administrative 상태	- resource 의 사용에 대해서 '사용' 또는 '금지'를 지정 가능 - resource 의 상태는 lock/unlock 으로 표현 가능 - unlock event 는 대응하는 resource 에 대한 object 의 관리 상태를 unlock - lock event 는 대응하는 resource 에 대한 object 의 관리 상태를 lock
Operational 상태에서 life cycle 상태	- 'not supported', 'pending active', 'post active' 상태는 'disable'로 map - 'active' 상태는 'enabled' 상태로 map

3. 시스템 설계

CNM 시스템은 ITU -T X.160 에서 제안하는 물리적인 구조를 제안하고 있다. CNM 시스템은 서로 다음 두개의 블록으로 구성되어 있다. 이 두개의 블록은 Customer 관리 시스템, 서비스 제공 시스템이다. 두 시스템 사이의 관리 정보의 교환은 CNM reference point 를 통한다. CNMC I/F 는 지원 프로토콜이 상호작용하는 경우에 적용되어져야 한다. CNMC 인터페이스는 OSI 의 CMIP(Common Management Information Protocol) 프로토콜에 기초를 두고 있다. 이것은 실시간 통지, 객체지향 기법, 재사용가능한 OSI 관리 소프트웨어 등의 개념에 기초를 두고 있다. CNMC 인터페이스는 customer domain 과 public domain 내의 여러 managed system 사이의 연결을 지원하는 역할을 수행한다.

CNME 인터페이스는 시간의 제약이 없고, 대화식 방식을 지원하지 않는다. 관리정보는 MHS(Message Handling System)프로토콜을 사용하여 EDI 메시지로 전송된다. 이처럼 CNM 시스템의 구조는 필요에 따라서 다양하게 변형이 가능하다.

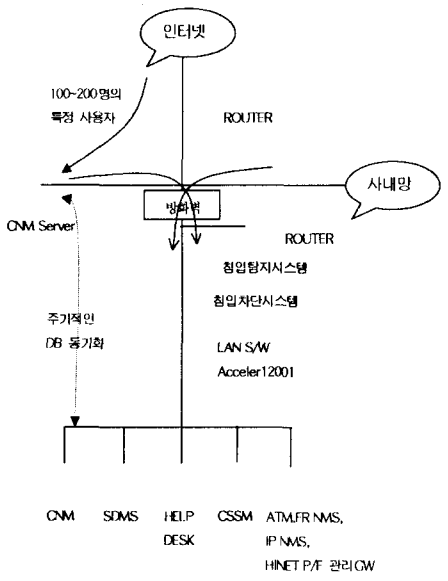
CNM 시스템의 보안 기능에 대한 설계 내용은 다음과 같다. 먼저 CNM 시스템의 보안 기능 제공을 위한 시스템 구조는 다음과 같다. CNM 시스템을 위한 보안 기능 설계 내용은 다음 그림과 같이 표현할 수 있다.

대부분의 CNM 시스템은 집중형 시스템 구조(centralized system)를 가지고 있다. 이러한 집중형 시스템은 여러가지 편리한 기능을 가지고 있는 반면에 여러가지 문제점도 수반하고 있다. 이러한 문제점으로는 CNM 시스템의 고장은 전체 네트워크에 치명적인 보안 결함을 유발할 수 있다. 이러한 문제를 해결하기 위하여 고장 감

내(fault tolerant) 기능을 갖는 시스템 구조가 바람직하다.

허가받지 않은 사용자의 접근을 막기 위하여 IDS(Intrusion Detection System) 프로그램을 설치한다. IDS 프로그램은 자체의 기능 다양화와 응용 프로그램 수준에서 key word 나 특정한 사용자, 특정한 단말기 등을 감시기능, 운영체제 커널 수준에서 감시, 감독 기능 구현을 통하여 해킹 자체가 원천적으로 무효화 되도록 한다.

원천적으로 허가받지 않은 사용자의 접근을 막기 위하여 방화벽(firewall)을 설치한다. 방화벽을 이중, 삼중으로 설치함으로써 각 시스템을 거칠 때 마다 사용 가능한 이용자인지 검증을 받도록 하고 있다. 그리고 방화벽에 보안 기능을 강화하기 위하여 방화벽의 등급 단계를 높이도록 한다. 이러한 초고속 통신망 시스템의 보안 구조는 다음 그림과 같다.



[그림 1] 초고속 통신망 보안 시스템 구조

[그림 1] 에서 CNM server 와 CNM 시스템은 동일한 데이타를 가진 백업 시스템이다. 따라서 이 시스템의 데이타에 대한 자료 일치성(data consistency) 을 보장하기 위한 실시간 자료 갱신이 필요하다. 그리고 사내망에서 CNM 방화벽을 통한 메인 시스템에만 접근이 가능하고 다른 통로는 모두 차단되어 있다. CNM server 에서도 마찬가지로 다른 네트워크 접근 경로는 차단되어 있고 메인 시스템에만 접근이 가능하다. 메인 시스템에 대한 접근 통제를 위하여 방화벽(firewall)과 IDS 를 설치하여 허가된 사용자만 접근이 되도록 한다. 인터넷 사용자는 CNM server 에만 접근이 가능하다.

4. 결론

초고속 정보통신망에서 CNM 시스템은 전체 네트워크에 대한 자원 관리, 기타 사용자 정보를 제공하는 시스템이다. 이 시스템은 네트워크를 통합 관리하는 시스템이기 때문에 관리에 신중을 기하지 않으면 네트워크 사용자들에게 치명적인 결과를 초래할 수 있다. 본 논문은 이러한 관점에서 CNM 시스템에 대한 외부 불순세력의 접근을 차단하기 위한 보안 기능의 설계에 초점을 맞추어 언급하였다.

CNM 시스템을 안전하게 관리하기 위하여 필요한 기능은 외부 인터넷에서 초고속 정보통신망 시스템으로 접근할 경우 방화벽을 설치하여 인증(허락)이 되지 않은 사용자를 걸러내는 작업을 한다. 이 방화벽은 K2 등급을 만족한다. 그리고 초고속통신망 시스템에서 CNM 시스템으로 접근할 때 외부 불순 세력의 침입을 탐지하기 위한 IDS 시스템을 가동한다. 그리고 CNM 시스템과 관리망 사이에 2 차 방화벽과 IDS 시스템을 설치함으로써 허가받지 않은 사용자의 접근을 차단한다.

앞으로 본 논문에서 제시한 시스템 구조를 실제 시스템에 구현하여 보안 기능을 만족하는 초고속 정보통신망 시스템 개발에 초점을 맞추어 진행할 예정이다.

참고문헌

[1] ATM Forum User-Network Interface Specification, Version 3.0.

[2] Internet Engineering Task Force RFC 1213, K. McCloghrie, M. Rose, " Management Information Base for Network Management of TCP/IP -based Internets: MIB-II" , 03/26/1991.

[3] TINA-C, " Service Architecture Version 5.0, " June 1997.

[4] ATM Forum af -nm-0019.000, " Customer Network Management (CNM) for ATM Public Network Service (M3 Specification) " , October 1994.

[5] ITU-T X.160, " Architecture for Customer Network Management Service for Public Data Networks ," October 1996.

[6] ITU-T X.161, " Definition of Customer Network Management Service for Public Data networks " , April 1995.

[7] ITU-T X.162, " Definition of Management Information for Customer Network Management Service for Public Data Networks to be used with the CNMs Interface," April 1995.

[8] IETF RFC 1155, " Structure and Identification of Management Information for TCP/IP -based Internets," May 1990.

[9] IETF RFC 1573, " Evolution of the Interfaces Group of MIB-II," January 1994.