논문 2006-43TC-7-13

# 차세대 네트워크 보안 표준화

## ( The Security Standardization for Next Generation Network )

오 행 석*, 김 정 녀*, 손 승 원*

( Heang-Suk Oh, Jeong-Nyeo Kim, and Sung-Won Sohn )

요 약

본 논문에서는 ITU-T SG 13 Q.15에서 현재 진행 중인 차세대 네트워크 보안 표준화 동향 및 관련 기술들에 대해 소개하고 있다. 차세대 네트워크 보안 관련 표준화는 차세대 네트워크 release 1에 대한 보안 요구사항과 차세대 네트워크 보안 가이드라인에 대한 기술 표준화 작업이 진행중이다. 우리나라에서도 차세대 네트워크 접근 제어를 위한 AAA 기술과 차세대 네트워크 단말기을 위한 사용자 인증 및 보안 플랫폼에 대한 표준화를 추진중이다.

Abstract

This paper introduces the security standardization trend and related technology in ITU-T SG 13 Q.15. Q.15 deals with the security requirements and guidelines over NGN(Next Generation Network) release 1. Korea proposes draft recommendation on "AAA(Authentication, Authorization and Accounting) Service for network access control over NGN" and .the procedure of the user authentication for the NGN convergence service terminals.

**Keywords :** 차세대네트워크, 보안요구사항, 보안 가이드라인, 보안 모델, 보안 위협

## Ⅰ. 서 론

인터넷 시대의 생활의 모습은 하루가 다르게 변화하고 있다. 기존 인프라를 통해서 고객의 다양한 취향에 맞춰 단기간에 신규서비스를 제공하기란 아주 어려운 실정이다. 또한 유무선망에 구애받지 않고, 시간과 장소에 상관없이 다양한 단말을 통해서 일정 수준 이상의 품질이 제공되는 서비스를 제공해야 하는 현실은 네트워크의 변화를 자연스럽게 유도하고 있다.

유선망의 경우, 불과 4-5년의 상황에 비해 연간 전화 통화량이 절반으로 감소세를 기록하고 있다. 이러한 상황은 앞으로 몇 년 사이에 기존 인프라를 통한 서비스 형태는 현저하게 위축되어 통신시장에서 경제적 이익을 창출하는데 어려움을 겪게 될 것이다.

차세대 네트워크(NGN : Next Generation Network)의 특성인 통신망과 서비스의 분리를 통한 유선. 무선. 방송 융합형 서비스로의 통신시장의 변화는 서비스 제공자에게 새로운 IP서비스 개발에 대한 동기유발 및 자극을 주기에 충분하다.

차세대 네트워크의 특징은 유연성(flexibility)과 비용절감(cost effective)이라고 정리할 수 있다. 통신사업자들은 단일망을 통하여 다양한 서비스를 제공, 효율적 투자 및 운용 유지보수를 통한 비용 절감, 서비스 개발 기간 단축을 통한 신속한 신규서비스 제공, 망의 유연성을 활용한 신속한 서비스 제공, 통합 멀티미디어형 고부가 서비스 제공, 이를 통한 신규 수익 창출을 차세대 네트워크 투자의 목적으로 여기고 있다.

ITU-T는 1995년부터 시작된 GII 프로젝트의 결과로 차세대 네트워크 표준화의 기반을 갖추고 하부 작업그룹인 SG13(Multi-protocol and IP-based networks and their internetworking)에서 2002년 6월 '차세대 네트워크 2004 프로젝트' 라는 차세대 네트워크 Focus Group을 결성하였으며 차세대 네트워크를 개발하기 위한 표준과 구현에 대한 정책의 수립과 관련된 활동을 조정하는 역할

* 정회원, 한국전자통신연구원 정보보호연구단
(ETRI, Information Security Division)
접수일자: 2006년6월15일, 수정완료일: 2006년7월14일

을 한다.

차세대 네트워크의 기능구조 모델에서는 구조와 프로토콜 부분의 표준화를 추진하게 되며 구조에서는 기존 단말기와 차세대 네트워크와의 상호작용 기능의 정의와 서로 다른 네트워크 사이의 단대단 서비스, 호 제어, 사용자의 이동성 지원 등에 대하여 연구 중에 있다. 또한 차세대 네트워크에서 사용되는 여러 가지 전송과 제어 프로토콜에 대한 내용도 다룬다.

네트워크 관리 부분에서는 오류·성능·사용자 관리, 요금·정산, 트래픽·경로설정 관리 등에 대한 표준화를 개발한다. 또한 차세대 네트워크는 구조, QoS, 네트워크 관리, 이동성과 상호 관련이 있기 때문에 혼합된 보안 구조를 가진다. 차세대 네트워크에서 사용 가능한 보안 정책을 개정하고 차세대 네트워크 보안 프로토콜과 보안 관련 API를 다룬다. SG 13는 15개의 Questions으로 구성되어 있으며, 차세대 네트워크 보안 관련 표준화는 Q.15에서 다루고 있다.

본 논문에서는 ITU-T에서 현재 진행 중인 차세대 네트워크 표준화 동향 및 관련 기술들에 대해 소개한다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 차세대 네트워크 보안 요구사항에 대해서 설명하고, Ⅲ장에서는 차세대 네트워크 보안 가이드라인을 소개한다. 결론으로 차세대 네트워크 보안 표준에 대한 국내 대응 전략을 제시하고자 한다.

## Ⅱ. 차세대 네트워크 보안 요구사항

차세대 네트워크 보안은 전송과 서비스 계층의 인터페이스에 관련된 요구사항을 제공하고 있다. 차세대 네트워크 전송과 서비스 계층에 대한 구조는 (그림 1)과 같다. (그림 1)에서 특정한 인터페이스 구간에서 보안 요구사항은 ITU-T Recommendation X.805에서 규정한 아래 항목을 적용하고 있다.

- 접근 제어(Access Control) : 접근 제어는 네트워크 자원을 허가 받지 않은 사용자로부터 보호하기 위한 보안 규정 항목이다. 접근 제어는 오직 허가 받은 사용자 또는 장치에게 네트워크 요소, 정보, 서비스, 응용에 접근을 허용한다.
- 인증(Authentication) : 인증은 통신 엔티티의 동일성을 확인을 위한 보안 규정 항목이다. 인증은 통신에 참여하고 있는 엔티티(사용자, 장치, 서비스 또는 응용)의 요구에 의한 동일성을 확인하는 절차이다.
- 부인 봉쇄(Non-repudiation) : 부인 봉쇄는 다양한 네트워크 관련 행위(의무(obligation), 의도(intent), 범행(commitment))의 유용한 증거를 만들어 데이터 관련한 특별한 행위 수행을 부정하는 것으로부터 사용자 또는 엔티티를 보호하기 위한 보안 규정 항목이다.
- 기밀성(Data Confidentiality) : 데이터 기밀성은 허가 받지 않은 노출(disclosure)에 대한 데이터를 보호하기 위한 보안 규정 항목이다. 데이터 기밀성은 허가 받지 않은 엔티티에 의해 데이터의 내용이 이해되지 않는 것을 보장한다. 암호화, 접근제어 목록 및 파일 접근 허가 등의 방법이 데이터 기밀성을 위하여 사용된다.
- 통신 보안(Communication Security) : 통신 보안은 허가 받은 종단점간의 정보 흐름(정보가 이들 종단점들 간에 사용되도록 방해 받지 않도록 함)을 보장하기 위한 보안 규정 항목이다.
- 무결성(Data integrity) : 데이터 무결성은 데이터의 정확성(correctness)과 정밀성(accuracy)을 보장하기 위한 보안 규정 항목이다. 데이터는 허가 받지 않은 행위로부터 수정, 삭제, 생성, 복사 등으로부터 보호 받아야 한다.
- 유용성(Availability) : 유용성은 네트워크의 침해로 인한 네트워크 요소, 정보, 정보 흐름, 서비스, 응용 등이 허가된 접근의 거부가 발생하지 않도록 보장하기 위한 보안 규정 항목이다. 재앙에 따른 복구도 이 범주에 해당된다.
- 비밀(Privacy) : 비밀성은 네트워크 행위의 관찰로부터 데이터를 보호하기 위한 보안 규정 항목이다.

### 1. 전송 계층에서의 보안 요구사항

#### 가. 차세대 네트워크 Customer 네트워크 구간

(1) Customer Gateway to Customer device

이 구간에서는 Data Confidentiality와 Authentication의 보호가 제공되어야 한다. 또한 Availability 보호가 보장되어야 한다.

(2) Customer device to Customer user

home user에 의한 home device의 Authentication이 확인되어야 한다. 또한 authorization과 Accountability가 요구된다.

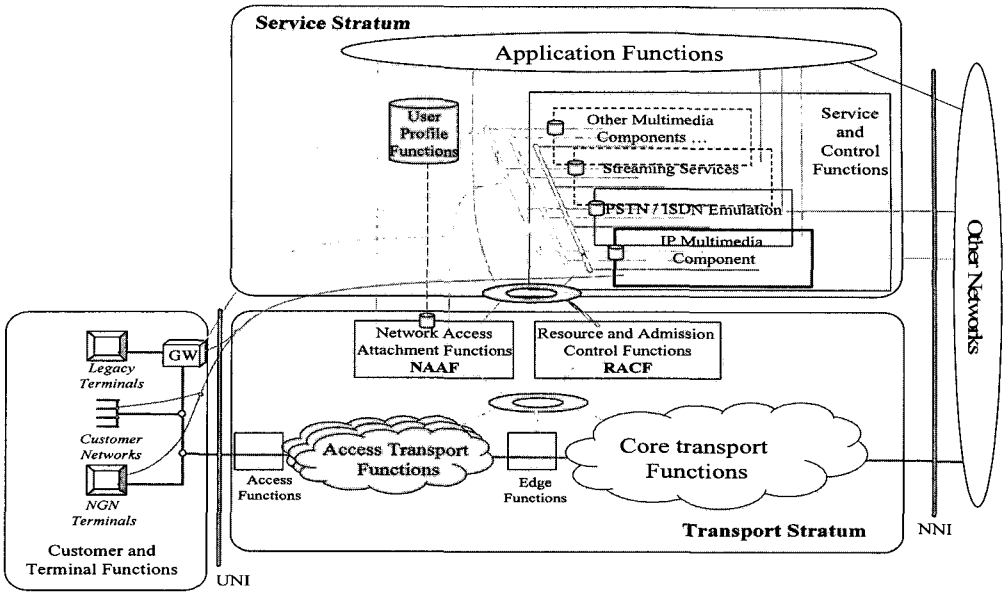


그림 1. 차세대 네트워크 보안 구조
Fig. 1. Security Architecture for Next Generation Network.

나. Customer network to IP-CAN (IP Connectivity Access Network) interface(UNI)

Customer network 구간에서의 요구에 대한 IP-CAN 자원 시용하기 전에 Access Control, Authorization, Authentication 등이 요구된다.

다. IP-CAN Function(UNI to INI or NNI)

Access 네트워크에 규정한 보안 요구사항이 IP-CAN 구간 전송 기능과 access signalling control system에 적용된다. 자원의 사용과 unauthorized access를 방지하기 위한 Access control과 authentication이 access network에서 요구된다. 자원은 Access 구간에서 네트워크와 서비스의 2 종류로 제어된다. 네트워크 접근을 위한 사용자 및 사용자 단말이 identify 되고 인증되어야 한다. 서비스의 access control은 service control function에 의해 제공된다.

라. Core Network function(INI - NNI)

Core 네트워크에 규정한 보안 요구사항이 Transport Network과 signalling control system(예, SIP(Session Initiation Protocol))에 적용된다. core network entity간에 Communication Security가 제공되어야 한다.

마. Customer Network to Customer Network Interface

(1) Remote user to customer gateway

표 1. 차세대 네트워크 전송 계층에서의 보안 요구사항
Table 1. Security Requirements in Transportation Stratum.

| 구간 | | 보안요구사항 | 비고 |
|---|---|---|---|
| 차세대 네트워크 Customer Network | Customer gateway to customer device | Data Confidentiality and Authentication, Availability | |
| | Customer device to customer use | Authenticity Authorization and accountability | |
| Customer Network to IP-CAN interface (UNI) | | Access control, Authorization and Authentication | |
| IP-CAN Function (UNI to INI or NNI) | | Access control and authentication | |
| Core Network function (INI - NNI) | | Communication security | |
| 차세대 네트워크 Customer Network to 차세대 네트워크 Customer Network Interface | Remote user to customer gateway | Data Confidentiality and Authentication, Availability, Data Integrity* | * 추가 |
| | Remote user to a device in customer network | Data Confidentiality, Data Integrity* | * 추가 |

불법 사용자로부터 Communication Interception를 방지하기 위하여 remote 사용자와 customer network 사용자가 Authentication되어야 한다. 또한 동시에 Data Confidentiality와 Availability가 확인되어야 한다.

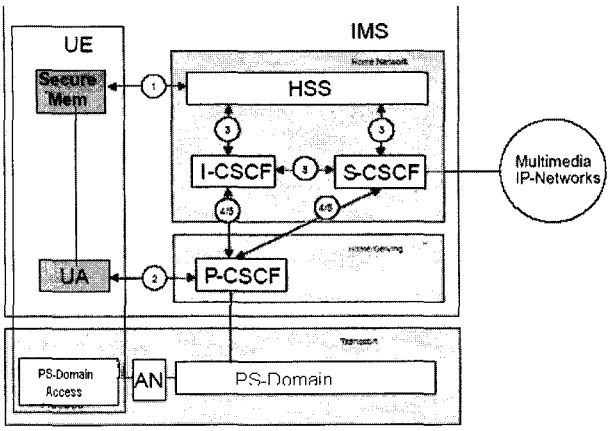


그림 2. IMS 보안 구조
Fig. 2. Security Achitecture for IMS

(2) Remote user to a device in customer network

불법 및 허가 받지 않은 사용자로부터 Communication Interception를 방지하기 위하여 remote 사용자는 Authentication되어야 한다. 또한 동시에 Data Confidentiality와 Availability가 확인되어야 한다.

## 2. 서비스 계층에서의 보안 요구사항

### 가. IMS core 네트워크 구조

IMS access security는 IP-CAN security에 의해 사용된 기술과 dependent 하지 않는다. IMS 사용을 위해 3GPP/3GPP2에 기반한 access security 기능이 제공되어야 한다. 3GPP는 authentication과 key 분배를 위하여 AKA(Authentication Key Agreement) 방법과 Smart card에 의존하고 있다. 3GPP2는 추가적인 option을 제공하고 있다. 차세대 네트워크 security를 위해서는 3GPP/3GPP2를 모두 수용해야 한다.

(그림 2)는 3GPP/3GPP2가 제공하는 IMS 보안 구조이다. security protection을 위해 서로 다른 5 종류의 인터페이스가 존재한다. 3GPP2에서 규정한 HSS(Home Subscriber Server)는 AAA server와 지원 기능 및 DB (예를들면, Home Location Register, Domain Name Server, Security and network access DB)를 포함한 logical entity로 정의한다.

### 나. IMS 보안 구조 인터페이스 요구사항

(1) 인터페이스 #1

UE와 S-CSCF간의 상호 인증이 제공되어야 한다. IMS access security는 IP-CAN security에 의해 사용된 기술과 dependent 하지 않는다. IMS security mechanism은 IP-CAN security mechanism과 독립적이어야 한다. UE와 HN간의 상호 인증이 제공되어야 한다. IMS security mechanism은 UICC (Universal Integrated Circuit Card)의 사용에 기반하고 있다.

표 2. IMS 서비스 계층에서의 보안 요구사항
Table 2. Security Requirements in IMS Service Stratum.

| 인터페이스# | 구간 | 보안요구사항 | 비고 |
|---|---|---|---|
| 1 | UE and the S-CSCF | Mutual authentication Authorization Authentication | |
| 2 | UE and a P-CSCF | Data origin authentication | |
| 3 | HSS and the S-CSC | Secure link | |
| 4 | P-CSCF resides in the Visited Network | Security | |
| 5 | P-CSCF resides in the HN | Security association | |

(2) 인터페이스 #2

SA(Security Association)을 보장하기 위한 UE와 P-CSCF간의 secure 연결이 요구된다. 수신한 데이터가 요구되로 되었는지 확인을 위한 데이터 인증이 요구된다.

(3) 인터페이스 #3

SA(Security Association)을 보장하기 위한 HSS와 S-CSCF간의 secure 연결이 요구된다.

(4) 인터페이스 #4

SIP capable node를 위한 다른 네트워크간의 security가 요구된다. P-CSCF가 VN(Visited Network)에 있을 때 적용되며, HN(Home Network)에 있을 때는 인터페이스 #5를 적용한다.

(5) 인터페이스 #5

SIP capable node를 위한 다른 네트워크간의 security가 요구된다. P-CSCF가 HN(Home Network)에 있을 때 적용된다.

# Ⅲ. 차세대 네트워크 보안 가이드 라인

차세대 네트워크 Security guideline은 기존의 ITU-T 권고안을 중심으로 차세대 네트워크를 위한 보안 모델을 제시하고, 차세대 네트워크 구현을 위한 통신 각 구성 요소(홈 네트워크, PSTN/ISDN evolution,

IMS 등)들의 보호를 위한 보안 모델과 항목을 제공하고 있다.

### 1. 보안 항목과 정의

- 신뢰성 있는 제3자 서비스/응용 제공자 : 네트워크 운용자에게 신뢰성 있는 부가가치 서비스 및응용 제공자로써 보안 신용도의 등급이 높다.
- 신뢰성 없는 제3자 서비스/응용 제공자 : 네트워크 운용자에게 신뢰성이 없는 부가가치 서비스 및 응용 제공자로써 보안 신용도의 등급이 낮다.
- 개방형 서비스/응용 플랫폼 : 부가 가치 서비스/응용을 위한 개방형 인터페이스로써 네트워크 운용자에 의해 제공되는 서비스/응용 플랫폼
- 책임(Accountability) : 엔티티의 행위가 엔티티에게만 추적되는 것을 보장하는 특성(ITU X.800 clause 3.3.3)
- 인증 : 수신된 데이터의 근원이 요구한 것과 같음을 확인(ITU X.800 clause 3.3.7)
- 인가 : 접근 권한에 근거한 접근의 허가(ITU X.800 clause 3.3.10)
- 기밀성 : 정보가 허가 받지 않은 사용자, 엔티티, 프로세서에 노출 또는 사용되는 것을 방지하는 특성(ITU X.800 clause 3.3.16)
- 무결성 : 데이터가 허용되지 않은 방법으로 변경 또는 폐기되지 않는 특성(ITU X.800 clause 3.3.16)
- 유용성 : 데이터가 허가 받은 엔티티의 요구에 의한 접근과 사용되는 특성(ITU X.800 clause 3.3.12)

### 2. 차세대 네트워크 위협 모델

차세대 네트워크 위협 모델과 기본적인 항목은 ITU-T 권고안에서 규정한 항목을 적용하고 있다.

- X.800 권고안 : 개방형 시스템간의 통신 보호가 요구되는 환경에 적용 가능한 일번적인 보안 관련 구조의 요소들을 정의
- X.805 권고안 : 종단간 네트워크 보안을 제공하는 네트워크 보안 구조를 정의

X.800과 X.805 권고안은 차세대 네트워크에 적용 가능한 다음의 보안 차세대 네트워크 위협 모델을 분류하고 있다. 이들 위협과 이들의 조합은 차세대 네트워크의 주요 공격 대상이다.

정보와 자원의 파괴

정보의 폐기(Corruption) 또는 변경

정보와 자원의 도난, 유출, 손실

정보의 노출

서비스의 가로채기(Interruption)

### 3. 차세대 네트워크 보안 요소

(표 3)은 보안 요소와 보안 위협의 매핑을 기술하고 있다. 여기에서 Y는 보안 요소에 의해 대립되는 보안 위협를 나타낸다.

### 4. 차세대 네트워크 보안 모델

차세대 네트워크 특징 중의 하나는 (그림 3)과 같이 계층(strata)과 면(plane)이 분리되어 있다. 또한 (그림 3)은 전송 계층과 서비스계층에 보안 연결(Association)을 보여주고 있다.

IP, IPsec과 MPLS LSP은 전송 계층의 Link Security 기능 위에 위치하며, 응용 기능은 서비스 계층의 TLS 기능 위에 위치한다. 각 응용과 TLS를 위한 보안 연결은 서비스 계층 보안을 제공한다. 보안 연결은 전송 계층의 IPsec에 의해 제공된다.

또한 (그림 3)은 사용자, 제어, 관리 평면(plane)을 기술하고 있다. 이들 평면은 네트워크 동작의 보호에 중점을 두고 있으며, 이들 간의 보안 보호(security protection)는 독립적이다.

표 3. 보안 요소의 보안 위협에 매핑
Table 3. The mapping between the security elements and threats

| 보안 요소 | 보안 위협 | | | | |
|---|---|---|---|---|---|
| | 정보파괴 | 정보폐기/변경 | 정보도난/유출/손실 | 정보 노출 | 서비스 가로채기 |
| 접근 제어 | Y | Y | Y | Y | |
| 인증 | | | Y | Y | |
| 부인 봉쇄 | Y | Y | Y | Y | |
| 기밀성 | | | Y | Y | |
| 통신 보안 | | | Y | Y | |
| 무결성 | Y | Y | | | |
| 유용성 | Y | | | | Y |
| 비밀성 | | | | Y | |

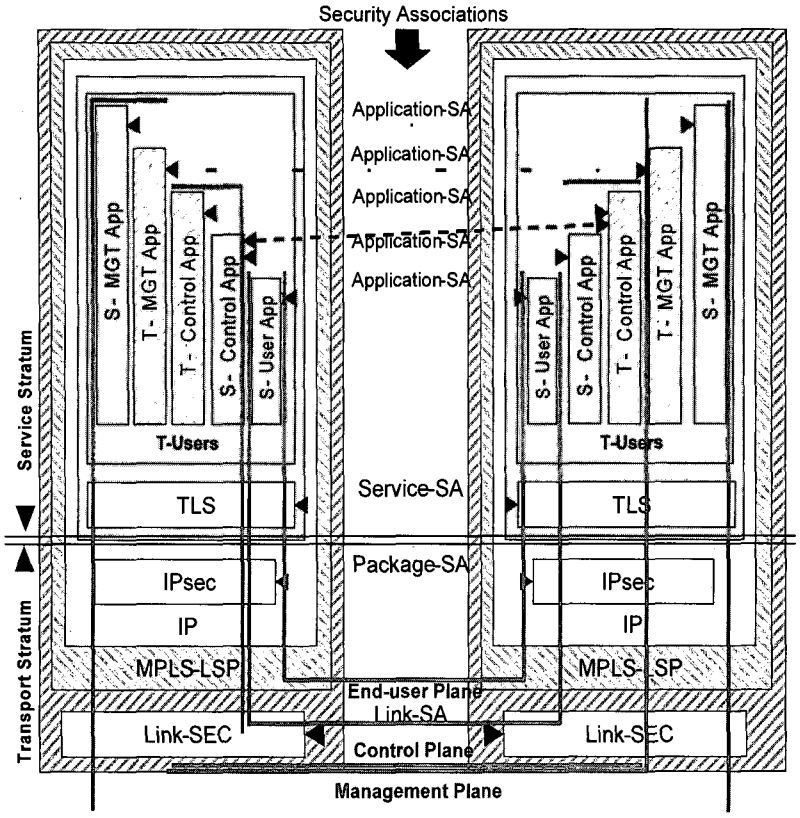


그림 3. 차세대 네트워크 보안 모델
Fig. 3. Security Model for Next Generation Network.

가. 사용자 측면 보안

종단 사용자 보안 측면은 서비스 제공자의 네트워크 사용과 접근 보안을 다루며, 종단 사용자의 데이터 흐름을 나타낸다.

나. 제어 측면 보안

제어 보안 측면은 네트워크를 통한 정보, 서비스, 응용의 전달을 가능하게 하는 동작의 보호에 중점을 두고 있다. 이는 라우터 또는 스위치가 전송 계층을 통하여 라우팅 또는 교환을 결정하게 하는 정보를 포함하고 있다.

다. 관리 측면 보안

관리 보안 측면은 네트워크 요소의 운용(operations), 경영(administration), 유지보수(maintenance) 규정(provisioning), 전송 능력, back-office systems 등의 보호에 중점을 두고 있다.

## 5. 차세대 네트워크 보안의 개념적 4 레이어 모델

차세대 네트워크 구조에서, 네트워크는 서비스 계층과 전송 계층으로 구분되어 있다. 서비스 계층은 응용 레이어와 서비스 레이어로 구성되어 있으며, 전송 계층은 패키지(Package) 레이어와 링크 레이어로 구성되어 있다.

가. 응용 레이어

응용 레이어는 서비스 제공자의 고객에 의한 네트워크 기반의 응용에 접근에 중점을 두고 있다. 응용은 웹 브라우징(web browsing), email, 파일 전송 응용 등을 포함하고 있다. 응용 계층에 적용된 보안은 고객과 네트워크의 보호에 적용한다.

나. 서비스 레이어

서비스 레이어는 서비스 제공자가 그들 고객에게 제공하는 다양한 서비스에 중점을 두고 있다. 서비스는 DNS(domain name services), 부가가치 서비스(value-added services), QoS 등을 포함하고 있다. 서비스 계층에 적용된 보안은 서비스 제공자와 그들 고객의 보호에 적용한다.

다. 패키지 레이어

패키지 레이어는 네트워크가 제공하는 전송 정보의 패키지 흐름에 다루고 있다. 차세대 네트워크에서 IP는 기존 서비스뿐만 아니라 종단 사용자에게 차세대 네트워크 서비스를 제공하는데 사용하는 기본적인 프로토콜이 될 것이다. 패키지 레이어에 적용된 보안은 IP 패키지 보호에 중점을 두고 있다.

라. 링크 레이어

링크 레이어는 직접적으로 연결된 네트워크간의 프레임 데이터 전송을 다루고 있다. 링크 레이어의 주요 역할은 전송 기능을 갖고 상위 레이어의 전송 에러를 줄이기 위함이다. 링크 레이어에 적용된 보안은 링크 프레임에 중점을 두고 있으며, 결과적으로 단일 링크 상의 보호를 제공하지는 않는다.

6. 차세대 네트워크 서브 시스템의 보안

본 절은 차세대 네트워크 서브 시스템의 보안을 제공하고 있다. 이들 서브 시스템은 각각이 의존적이지만, 여기서는 각 서브 시스템의 본안을 개별적으로 다루고 있다.

가. IP-CAN

IP-CAN 보안은 미디어와 신호를 위한 전송을 제공하는 IP-CAN 구조에 의해 제공된다. 이 보안 구조는 IMS에 의해 규정된 보안에 직교(orthogonal)한다. IP-CAN 보안은 기밀성(confidentiality)을 제공해야 한다. 기밀성은 IPsec의 ESP(encapsulation security payload)인 네트워크 레이어 보안 메카니즘에 의해 얻어진다. IPsec은 전송 모드에서 호스트간 또는 터널 모드의 라우터간에 동작하는 종단간 프로토콜이다.

나. IMS 네트워크 영역과 IMS-to-non-IMS 네트워크 보안

IMS 기능적인 엔티티는 코아 네트워크내의 물리적인 엔티티에 의해 실현된다. 즉 네트워크 엔티티내의 상호연결(interconnection)이 보호되어야 한다. 네트워크 영역 보안은 데이터와 신호를 보호한다. 보안은 IPsec ESP에 기반을 두며, 3GPP/3GPP2 규격과 일치하여야 한다.

IMS-to-non-IMS(예, 차세대 네트워크의 IMS 서브 시스템과 차세대 네트워크의 다른 서브 시스템간) 네트워크 인터페이스를 위한 보안은 데이터와 신호를 보호한다. 이러한 보안은 TLS 프로토콜에 기반하여야 한다. 사용자 데이터 인증은 Wi-Fi와 LAN 접근을 위한 연결상에서 로밍을 지원할 목적으로 다른 네트워크 영역에서 유용하여야 한다. 베어러 레벨 서비스는 SRTP (Secure Real-time Transport Protocol)에 의해 제공되어야 한다.

다. IMS 액세스

IMS 사용자는 IMS 사용의 권한을 부여 받아야 한다.

라. 응용

차세대 네트워크 상에 제공되는 응용은 각각 자신의 보안 요구사항을 가져야 한다고 규정하고 있다.

마. 차세대 네트워크 상의 개방형 서비스/응용 프레임워크

개방형 서비스/응용은 차세대 네트워크 구조에서 가장 중요한 특성중의 하나이다. 제3자 서비스/응용 사업자는 부가가치 서비스/응용을 개발하기 위하여 개방형 서비스/응용 플랫폼에서 제공되는 API를 사용한다. 네트워크 제공자의 신용 등급에 따라, 부가가치 서비스/응용 사업자는 네트워크 제공자에 의해 신용 사용자와 그렇지 않은 사업자로 분류하다. 전자는 네트워크 제공자이거나, 네트워크 운영자에 의해 신뢰성이 높은 서비스/응용 사업자로 간주되는 자회사 또는 합자회사이다. 후자의 경우는 신뢰성이 없이 서비스/응용을 제공하는 독립적인 서비스/응용 사업자이다.

차세대 네트워크는 개방형/분산형 제어 구조이므로, 개방형 서비스/응용 플랫폼과 부가가치 서비스/응용에 다양한 위협(정보의 파괴/변경/노출, 서비스/응용의 가로채기 등)이 존재한다. 차세대 네트워크에서 개방형 서비스/응용 플랫폼과 부가가치 서비스/응용을 보안 위협으로부터 보호하는 것은 필요하다.

(그림 4)는 일반적인 개방형 서비스/응용 프레임워크의 보안 모델을 보여주고 있다. 이는 개방형 서비스/응용 프레임워크간의 다양한 차원(dimensions)을 보여 주고 있다. 보안 기능은 서비스/응용과 통신의 보호를 보장한다. 응용의 시나리오에 따라, 서비스/응용 제공자는 보안 기능의 배치를 위하여 다른 보안 차원의 사용이 요구된다.

부가가치 서비스가 제3사업자에 의해 신뢰성 있게 제공되는 경우, 제3자 사업자로부터 서비스/응용 플랫폼으로 전송되는 컨텐츠를 모니터링과 필터링이 필요없

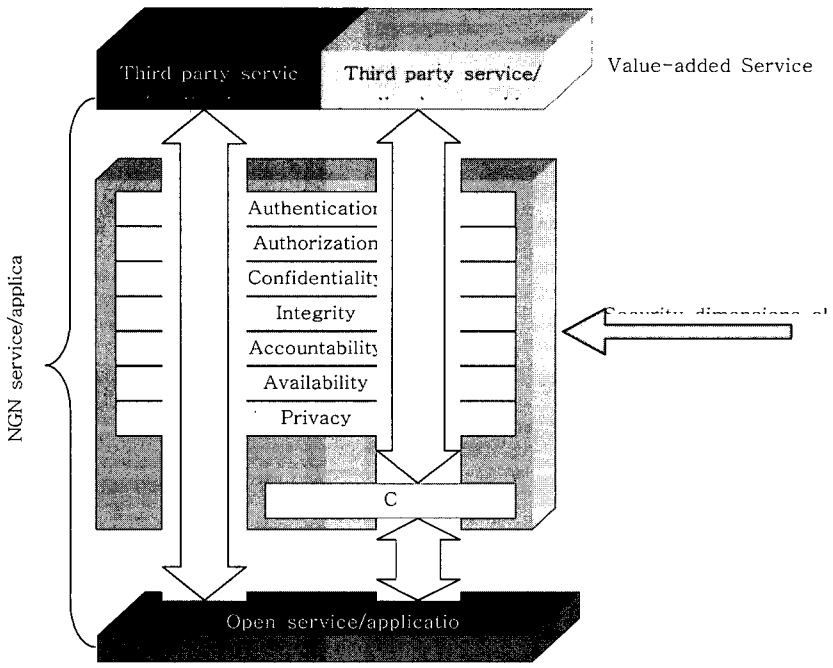


그림 4. 차세대 네트워크 서비스/응용 프레임워크의 보안 모델
Fig. 4. Security Model for NGN Service and Application Framework.

다. 정보가 개방형 네트워크를 통하여 전송되는 경우, 정보의 무결성과 기밀성이 보장되어야 한다. (그림 4)의 * 마크는 신뢰도 있는 제3자에게는 선택적(인증, 허가, 비밀성 등)이다.

부가가치 서비스가 제3사업자에 의해 신뢰성 없게 제공되는 경우, 제3자 사업자로부터 서비스/응용 플랫폼으로 전송되는 컨텐츠의 모니터링과 필터링이 요구된다. 데이터의 보호를 위한 기밀성이 보장되어야 한다. 유용성, 무결성, 비밀성도 다른 네트워크 상태에서 보장되어야 한다.

### 바. PSTN/ISDN evolution

PSTN/ISDN evolution의 보안 요구사항은 2005년 8월 제네바의 FG차세대 네트워크의 회의에서 처음 논의되었으며, 다음 회의까지 기고서의 주요 내용을 차세대 네트워크 보안 가이드라인에 추가키로 결정하였다. PSTN/ISDN이 차세대 네트워크로 전이함에 따라 기존 네트워크에서 존재하지 않은 보안에 대한 위협에 직면하게 된다. PSTN/ISDN evolution의 보안 요구사항에서는 보안 위험 요소와 해결책을 제시하고 있으며, 이의 주요 내용은 (표 4)과 같다.

표 4. VoIP 취약성
Table 4. The Weakness for VoIP.

| 취약성 | 위협 | 대응책 | 시나리오 |
|---|---|---|---|
| 신호 게이트웨이 | - Denial of service<br>- Service 남용 | - ISUP 모니터링<br>- 남용 감시 시스템 | PSTN emulation |
| 취약한 인증 | - Impersonating(위장)<br>- 프라이버시 파괴 | - 외부 인증 기술<br>- Private call tunneling | PSTN emulation |
| 무결성의 부족 | - 호 가로채기<br>- 신호 변경<br>- Denial of service | - Private call tunneling | PSTN simulation |
| 기밀성 부족 | - 호 가로채기<br>- 프라이버시 파괴 | - Private call tunneling | PSTN simulation |
| IP 네트워크 공격에 취약 | - Denial of service<br>- 프라이버시 파괴<br>- 서비스 남용 | - 호 서버 엔티티로부터 종단 사용자 분리<br>- 침입 방지 시스템 개발 | PSTN emulation/simulation |

사. ETS(Emergency Telecommunications Services)

ETS의 보안 요구사항은 2005년 8월 제네바의 FG차세대 네트워크의 회의에서 처음 논의되었으며, 다음 회의까지 기고서의 주요 내용을 차세대 네트워크 보안 가이드라인에 추가키로 결정하였다.

차세대 네트워크에서 ETS의 보안과 유용성은 다음과 같다.

- 일반 차세대 네트워크 보안 - 차세대 네트워크 액세스/전송 서비스/응용 서비스의 보안을 지원하는 완화 능력, 메카니즘과 정책을 제공
- ETS 보안 - ETS 보안을 지원하는 완화 능력, 메카니즘과 정책을 제공하며, 특별한 고려가 요구되는 (예, DoS(denial of service) 공격) 등에 보안 서비스가 우선 먼저 처리되어야 함
- 차세대 네트워크에서 ETS 사용자의 인증과 허가가 요구됨

아. HN(Home Network)

2005년 8월 제네바의 FG차세대 네트워크의 회의에서는 차세대 네트워크에서의 HN 보안 요구사항는 ITU-T SG13의 연구범위가 아니므로, 이에 대한 가이드라인을 기술문서에서 삭제키로 합의하였다. HN 보안 표준화는 ITU-T SG17에서 진행중이므로 이를 참조키로 하였으며, ITU-T SG13에서는 차세대 네트워크와 HN과의 접속에 필요한 보안 요구사항을 도출하여 기술문서에 보완키로 하였다.

## IV. 결 론

본 논문에서는 ITU-T SG 13 Q.8 네트워크 보안 그룹에서 진행중인 차세대 네트워크 Security에 대한 표준화 동향을 기술하였다. 차세대 네트워크 보안 표준화는 주로 차세대 네트워크 보안을 위한 요구사항과 Guideline 제시를 위한 기술 문서 작성을 진행하고 있다. 차세대 네트워크 보안 표준화는 2005년 7월 회의에서 SG 13내의 WP 2의 Q.15로 정식 과제로 선정되어 추진키로 결정되었다. 현재 표준화는 미국의 Lucent, 캐나다의 Nortel, 영국의 BT 등이 주로 활동하고 있다.

한국의 경우 2006년 1월 회의부터 차세대 네트워크 접근 제어를 위한 AAA 서비스의 표준화를 주도적으로 추진하고 있다. 또한 국내 BcN 기술을 차세대 네트워크 단말기 표준에 참여하여 사용자의 인증 및 보안 플랫폼에 대한 국제 표준화를 추진 중에 있다. 이에 국내 보안 관련 연구소, 학계, 산업계에서 BcN 보안 표준을 마련하여 차세대 네트워크 보안 분야에 국제 표준을 선점 할 수 있는 기반 마련이 시급하다.

## 참 고 문 헌

[1] ITU-T SG 13 FG차세대 네트워크-OD-00132
[2] ITU-T SG 13 FG차세대 네트워크-OD-00133
[3] ITU-T Recommendation X.805
[4] 3GPP TS 33.102, *3G Security; Security Architecture*
[5] 3GPP TS 33.103, Universal Mobile Telecommunications System (UMTS); 3G Security Integration Guideline
[6] http://www.itu.int/

## 저 자 소 개


오 행 석(정회원)
1981년 한양대학교 공과대학 학사 졸업
1983년 한양대학교 대학원 석사 졸업
1997년 충북대학교 대학원 박사 졸업
1983년~현재 한국전자통신연구원 정보보호 연구단 정보보호원천연구팀 책임연구원
<주관심분야 : 컴퓨터 네트워크 보안, 프로토콜 공학>

김 정 녀(정회원)
1987년 2월 전남대학교 전산통계학과(이학사)
1995년~1996년 Open Software Foundation Research Institute 공동 연구 파견 (미국)
1998년 3월~2000년 2월 충남대학교 대학원 컴퓨터공학과 (공학석사)
2000년 3월~2004년 2월 충남대학교 대학원 컴퓨터공학과 (공학박사)
2005년~2006년 박사후연수(미국 UCI)
1988년 2월~현재 한국전자통신연구원, 정보보호원천연구팀장(책임연구원)
<주관심 분야 : OS, Secure OS, System & Network Security>

손 승 원(정회원)
1984년 경북대학교 전자공학과 학사 졸업.
1994년 연세대학교 전자공학과 석사 졸업.
1999년 충북대학교 박사졸업
1983년~1986년 삼성전자(주) 연구원
1986년~1991년 LG전자(주) 중앙연구소 팀장
1991년~현재 한국전자통신연구원 정보보호 연구단 단장/책임연구원
<주관심분야 : 네트워크 정보보호, RFID/USN정보보호, 유비쿼터스 정보보호, 정보보호 정책>