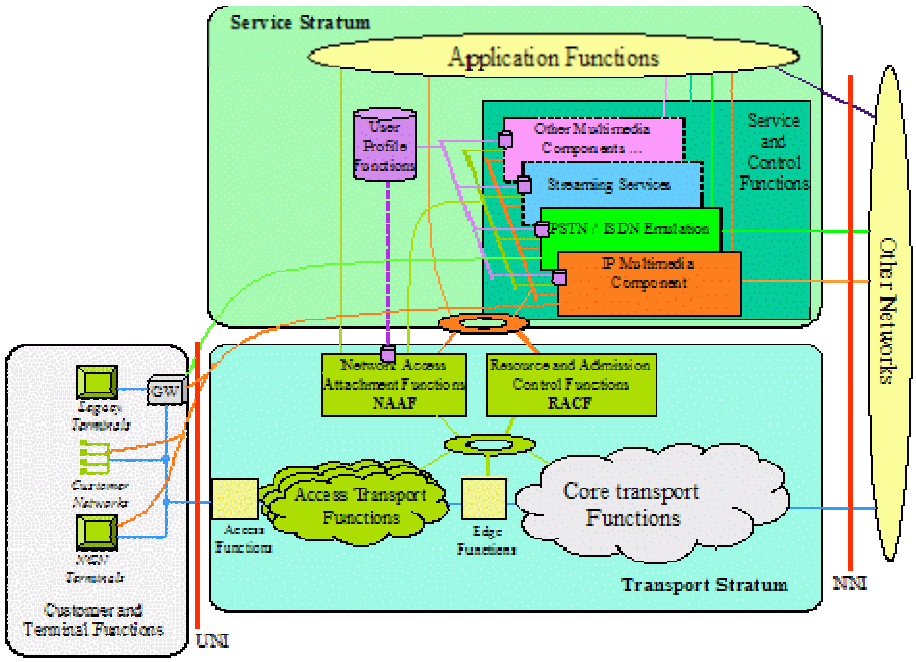
[정보보호] NGN 보안을 위한 표준화 동향

NGN(Next Generation Network)은 패킷 기반의 통신 서비스를 제공하기 위한 네트워크로서, 광대역 고속 통신이 가능하고, 처리능력 및 전송 지연 등의 서비스 품질이 보장되며, 전달 기술과 서비스 기술이 독립적이며, 완전한 이동성을 지원하는 ITU-T가 개발중인 차세대 통신망이다. NGN은 그림 1과 같이 트래픽 전달 측면에서 코어 전달 기능과 액세스 전달 기능으로 구성되며, 자원 및 서비스 제공 측면에서 사용자에게 종단간 연결을 위한 전달 계층(Transport Stratum)과 타 망과의 연결과 멀티미디어 서비스 제공을 포함한 응용 서비스를 다루고 있는 서비스 계층(Service Stratum)으로 구분될 수 있다. NGN은 기존의 별개 망으로 운영되는 유선망과 무선망이 하나로 통합된 액세스 망과 코어 전달망을 통하여 인터넷 전화 서비스(VOIP, Voice over IP), 방송 서비스 등의 다양한 멀티미디어 서비스까지를 제공할 수 있는 컨버전스 망이라고 할 수 있다. 따라서 음성 서비스는 물론 멀티미디어 서비스와 인터넷 서비스가 동시에 제공될 수 있다. 현재 ITU-T에서는 NGN을 위한 기술과 표준을 개발하고 있으며, NGN 보안 표준은 여러 SG들이 협력하여 개발하고 있다. 본 고에서는 NGN 보안을 위한 활동 현황을 살펴보고, 이를 근거로 향후 표준화 항목을 살펴본다.



<그림 1> NGN 전달 및 서비스 계층 구조

NGN 보안 위협

NGN에서의 보안 위협은 크게 (1) 사용자 관점에서 메시지의 도청, 패스워드 등의 중요 기밀 정보의 도난 및 손실, 원하지 않은 스팸, 아이디 도용, 바이러스/웜/스파이웨어로부터의 단말 오염, 사용자에 대한 프라이버시 손실, 서비스 가용성 부재, 그리고 공격자에 의한 과도한 트랙픽 집중을 통한 단말에 대한 트래픽 플러딩(flooding) 공격 등이 있으며, (2) 서비

스 제공자 관점에서 서비스의 도용, 서비스 거부 공격 등의 망에 대한 사이버 공격, 네트워크 구조의 인가되지 않은 공개, 그리고 비인가된 네트워크 설정 및 구조 변경 등이 있다. 이외에 정확히 위협이라고는 할 수 없으나 멀티미디어 서비스를 제공하기 위한 방화벽 등의 망설비의 설정 변경 등이 요구되고 있다. NGN 보안은 이러한 위협을 제거하는 여러 가지 대책이 강구될 것이다.

표준화 추진 현황 및 내용 개요

현재 ITU-T에서 NGN을 위한 보안 표준은 NGN 보안표준을 주도하는 SG13, 보안 활동을 주도하고 있는 SG17, 그리고 망관리 측면의 보안 문제를 다루는 SG4, 신호 방식과 신호 채널에 대한 보안을 표준화하고 있는 SG11, 그리고 멀티미디어 보안을 개발하고 있는 SG16에서 분산적이고 협력적으로 개발되고 있다. SG4에서는 연구과제 7에서 통신망 관리에 대한 인터페이스에 대한 보안 요구사항을 정의하고 있고, SG11에서는 연구과제 7을 중심으로 신호 방식을 위한 액세스 보안을 정의하고 있으며, SG13에서는 연구과제 15를 중심으로 보안 일반 및 인증 요구사항과 보안 가이드라인을 정의하고 있으며, SG16에서는 연구과제 25을 중심으로 인터넷 컨퍼런스를 위한 ID 인증관리 구조인 ID 페더레이션 등에 대한 표준을 정의하고 있다. SG17에서는 연구과제 5, 6, 7, 9를 중심으로 NGN을 위한 인증 및 키관리 프레임워크에 대한 표준화, 사이버 보안 가이드라인, 정보보호 관리 체계, 그리고 안전한 패스워드 인증 가이드라인 등에 대한 표준을 각각 추진하고 있다. NGN을 개발하기 위하여 ITU-T 외부 표준화 기구는 ETSI, IETF, ATIS, ISO/IEC SC27, 3GPP, 3GPP2 등 대부분의 국제 표준화 단체가 협력하여 NGN을 개발하고 있다. 특히 ETSI의 TISPAN(Telecommunications and Internet converged Services and Protocols for Advanced Networking)에서는 위험 분석 등의 보안 표준이 개발되었으며, 이의 수용 여부가 주목되고 있다.

현재 ITU-T가 개발 중인 대표적인 NGN 보안 표준은 지난 2004년 6월에 시작하여 2005년 11월에 활동을 종료한 포커스그룹 NGN(Focus Group NGN)의 결과 문서로 현재 SG13으로 이전하여 보완 개발 중인 NGN 보안 요구사항 문서와 NGN 보안 가이드라인 문서가 있다. 보안 요구사항에서는 NGN 이 가져야 할 기본 보안 요구사항을 제시하고 있으며, 구체적으로 키 관리 기능이 제공되어야 한다는 일반 보안 원칙 등을 기술한 일반 보안 요구사항, 확장 가능한 보안 구조를 가져야 한다는 일반 보안 목표, 기본적으로 요구되는 보안 서비스를 정의한 보안 서비스 정의, 전달 계층의 보안 요구사항, 서비스 계층의 보안 요구사항을 다루고 있다. 먼저 서비스 계층의 경우, (1) 멀티미디어 서비스를 제공하는데 필요한 IMS(IP Multimedia Service) 코어 망 보안구조, (2) 보안 구조에서 인터페이스에 대한 보안 요구사항을 다룬 IMS 보안 구조 인터페이스 요구사항, (3) 서비스 및 자원 제어 서브시스템 간에 보안 문제를 다룬 코어 네트워크의 전달 영역 보안, (4) 자원에 대한 응용 요구에 응답하기 이전에 접근제어 및 인증의 문제를 다루는 응용 보안, (5) NGN을 통한 인터넷 전화

(VOIP, Voice over IP) 트래픽에 대한 기밀성과 사용자 ID 보호 등의 문제를 다루는 VOIP 보안, (6) 재난 상황에 대비한 위기 통신망 서비스와 재난복구 통신망 보안, (7) 공개 서비스 플랫폼 및 부가가치 서비스 간에 보안 등의 보안 요구사항 등을 다루고 있다. 전달 계층의 경우, 보안 요구사항은 (1) 가입자 장치와 가입자 게이트웨이 간에 가입자 댁내 보안, (2) NGN 액세스 망인 IP-CAN(IP-Connectivity Access Network) 자원 요구를 위하여 필요한 인증 및 접근제어 등의 보안 기능 요구사항을 제시한 가입자 망과 IP-CAN간에 인터페이스 보안, (3) 네트워크 장치와 신호 장치에 대한 보안 요구사항에 대한 코어 전달망 보안, (4) 원격 가입자의 홈 게이트웨이로의 원격 인증과 인가에 대한 원격 NGN 가입자 보안 등에 대한 보안 요구사항을 다루고 있다.

안전한 NGN을 구축하기 위한 일반 보안 원칙과 세부 보안 가이드라인에 대하여 기술하는 NGN 보안을 위한 가이드라인은 (1) NGN 보안 위협과 보안 대책, (2) 응용, 서비스, 패킷, 그리고 링크 계층으로 구성되는 4 계층 기반 보안 모델과 보안 연관, 그리고 (3) 구성 서브시스템에 대한 보안 등에 대한 기본 가이드라인을 기술하고 있다. 구성 서브시스템 보안의 경우, (1) 트래픽의 전달과 신호 전달을 담당하는 IP-CAN 서브시스템에 대한 네트워크 계층 보안, 링크 계층 보안, 그리고 확장 가능한 인증방식에 대하여 기술하고 있는 IP-CAN 서브시스템 보안 가이드라인, (2) IMS 데이터와 신호에 대한 보안, 베어러 서비스를 보호하기 위한 안전한 실시간 전달 프로토콜(SRTP, Secure Real Time Protocol) 사용, 로밍 서비스를 지원하기 위한 사용자 인증 데이터의 활용, 종단계층 보안 프로토콜인 TLS(Transport Layer Security) 프로토콜, IETF 망계층 보안 프로토콜인 IPSec 프로토콜의 사용을 권하는 IMS 네트워크 영역 및 IMS와 비-IMS간에 보안 가이드라인, (3) IMS 사용자 인증, IMS 보안 구조 하에서 각 구성 서브시스템 간에 보안 가이드라인을 기술하는 IMS 접근 보안 가이드라인, (4) 부가가치 서비스와 공개된 플랫폼 간에 제공되어야 할 보안 서비스를 정의하고 있는 공개 플랫폼 보안 가이드라인, (5) 긴급 통신망 서비스와 재난관리 통신망을 위한 가이드라인, (6) IMS 트래픽의 기존 NAT나 방화벽을 통과하는 문제를 다루는 NAT/방화벽 통과를 위한 가이드라인으로 구성되어 있다.

표준 기술 도출 및 향후 추진사항

SG13의 연구과제 15에서는 보안 요구사항, 인증 요구사항, AAA 요구사항, 보안 가이드라인, 그리고 기타 세부 보안 기술을 표준화할 것이고, SG17의 연구과제 5에서는 NGN을 위한 인증 및 키관리 프레임워크를 개발할 것이며, SG11에서는 신호 방식을 위한 액세스 보안 표준을 개발할 예정이다. 현재까지의 표준화 실적을 근거로 NGN을 위하여 향후에 개발되어야 할 주요 표준화 항목은 다음과 같이 도출될 수 있다.

- NGN에 적용 가능한 암호 알고리즘 슈트(타원곡선 암호 알고리즘 슈트 포함)
- 확장 가능한 인증방법, AAA(Authentication, Authorization and Accounting) 프로토

콜, 기타 요소 암호 프로토콜 등에 대한 기본 암호 프리미티브
- 최종 사용자와 네트워크 요소를 위한 사용자 친화적인 키 분배 및 관리
- 터미널 이동성과 네트워크 이동성을 위한 공개키 기반구조를 포함한 인증 기반구조
- NGN을 통하여 사용자 및 기기의 위치 추적을 막기 위한 사용자 및 네트워크 프라이버시 보호
- 멀티미디어 서비스를 위한 IMS 서비스 제공을 위한 보안 가이드라인
- NGN 코어 네트워크 보호하기 위한 능동적인 침입 탐지 및 차단을 포함한 보안 가이드라인
- IETF에서 표준화한 IPSec, TLS, SRTP 등의 기존 보안 프로토콜의 적용 및 구현을 위한 가이드라인
- DSL(Digital Subscriber Loop), WLAN(Wireless LAN), 케이블 접근 망 시나리오를 위한 액세스 망을 위한 보안
- NGN을 통하여 등급화된 보안 서비스를 제공하기 위한 보안 정책 가이드라인
- 인터넷 멀티미디어 응용 세션 개시 프로토콜을 위한 홉대홉 및 종단간 SIP(Session Initiation Protocol) 보안
- NGN 재난복구와 위기 관리를 위한 가이드라인
- NGN을 통한 N-RFID(Networked Radio Frequency ID) 보안
- 실시간 응용을 위한 NAT/방화벽 통과 문제

향후에는 도출된 내용을 중심으로 각 SG들간의 적절한 역할 분배를 통하여 NGN 보안 표준이 개발될 것으로 예측되며, ETSI의 TISPAN과 IETF 등의 국제 표준화 기구간의 협조 하에 추진될 것이며, 특히, SG13에서는 보안 요구사항 및 가이드라인을 중심으로, SG17에서는 세부 보안 핵심 기술을 중심으로, SG11에서는 신호 방식 보안을 중심으로 수행될 예정이다.

염흥열(순천향대학교 교수, Rapporteur, Q.9/17, ITU-T, hyyoum@sch.ac.kr)