차세대 네트워크 보안 표준화 동향

오 행 석

한국전자통신연구원

목 차

Ⅰ. 서 론

차세대 네트워크(NGN: Next Generation Network)의 특징인 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 internetwor- king)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 역할을 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 16개의 Questions으로 구성되어 있으며, 차세대 네트워크 보안 관련 표준화는 Q.15에서 다루고 있다.

본 논문에서는 ITU-T SG13 Q.15에서 개발된 권고안을 중심으로의 차세대 네트워크 보안 표준화 동향 및 관련 기술들에 대해 소개한다. 본 논문의 구성은 다음과 같다. 2장에서는 차세대 네트워크 보안 요구사항에 대해서 설명하고, 3장에서는 차세대 네트워크 인증 요구사항, 4장에서는 차세대 네트워크 AAA 서비스의 권고 표준안을 소개한다. 결론으로 차세대 네트워크 보안 표준에 대한 국내 대응 전략을 제시하고자 한다.

Ⅱ. 차세대 네트워크 보안 요구사항

안전 위협에 대한 NGN 인프라를 위한 보안 요구사항을 제공한다. 이는 국제표준 권고안 X.805의 원칙을 적용한다. (그림 7-1)은 ITU-T SG13에서 NGN의 정보보호 모델 개발을 위한 표준 규격으로 활용되고 있다. 이는 크게 보안계층, 보안평면 및 8개의 보안 서비스로 구성되어 있다. 보안 계층은 네트워크 장치 및 시설들의 계층별 분류로 인프라계층, 서비스계층, 응용계층으로 분류한다. 보안평면은 네트워크 행위별 분류로 관리평면, 제어평면, 사용자평면으로 분류한다. 각 보안평면은 각 보안계층별로 적용하여 네트워크 서비스의 보호대상을 상세하게 도출한다. (그림 1)에서 특정한 인터페이스 구간에서 보안 요구사항은 ITU-T Recommendation X.805에서 규정한 8가지 정보보호 기능 - 접근제어, 인증, 부인방지, 비밀성, 통신흐름 보호, 무결성, 가용성, 프라이버시로써 보호 대상별로 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) : 통신보안은 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.

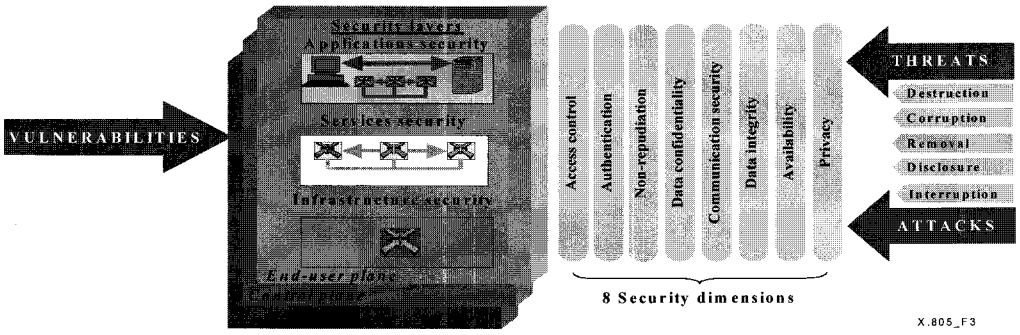

그림 1. NGN 정보보호 참조 모델

차세대 네트워크 Security는 전송과 서비스 계층의 인터페이스에 관련된 보안 요구사항을 제공하고 있다.

2-1. 전송 계층에서의 보안 요구사항

2-1-1. 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.

2-1-2. 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.

2-1-3. 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.

2-1-4. Core Network function(INI - NNI)

Core 네트워크에 규정한 보안 요구사항이 Transport Network과 signalling control system(예, SIP(Session Initiation Protocol))에 적용된다. core network entity 간에 Commun- ication Security가 제공되어야 한다.

2-1-5 Customer Network to Customer Network Interface

① Remote user to customer gateway
불법 사용자로부터 Communication Interception를 방지하기 위하여 remote 사용자와 customer network 사용자가 Authentication 되어야 한다. 또한 동시에 Data Confidentiality와 Availability가 확인되어야 한다.

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.

표 1. 차세대 네트워크 전송 계층에서의 보안 요구사항

구 간		보안 요구사항	비 고
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

2-2. 서비스 계층에서의 보안 요구사항

2-2-1. 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.

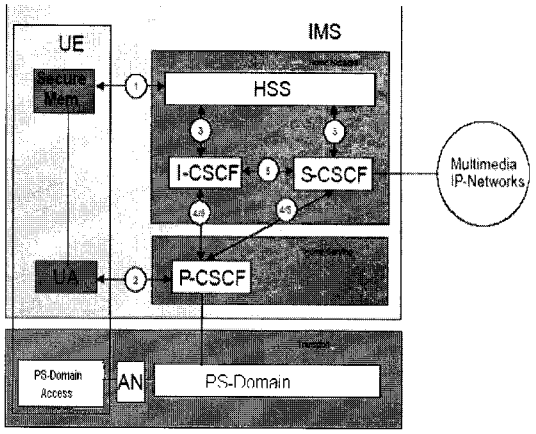

그림 2. IMS 보안 구조

그림 2는 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.

2-2-2. 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.

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.

표 2. IMS 서비스 계층에서의 보안 요구사항

인터페이스 #	구 간	보안 요구사항	비 고
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	

III. 차세대 네트워크 인증 요구사항

3-1. 보안 위협과 위험성

NGN을 구성하는 시스템, 인터페이스, 정보, 자원, 통신요소(신호, 트래픽 등) 및 서비스가 보안 위협에 노출되어 있다. NGN에 위협 요소는 다음과 같다.

- 비인가자의 수색(네트워크의 약점을 찾기 위한 시스템의 원격 분석)
- 정보의 손상 또는 수정
- 정보와 다른 자원의 절도, 제거, 손실 및 파괴
- 정보의 공개
- 서비스의 인터럽션과 서비스의 거부

또한 NGN은 PSTN 환경과 다른 환경에서 작동할 것이고, 그러므로 내부 또는 외부로 부터 위협과 공격의 다양한 타입에 노출될 수 있는 것은 명백하다.

NGN은 네트워크와 사용자 구내 설비를 불안전하게 하기 위해 연결성과 관련되는 것으로 신뢰되지 않고 신뢰성 네트워크와 단말기에 직접적이거나 간접 연결성을 가질 것이고, 그러므로 보안 위험과 위협에 노출될 것이다. 예를 들면, NGN은 (그림 7-2)에 나타난 바와 같이 직접적이거나 간접적이게 (즉, 또 다른 네트워크를 통하여) 연결할 수 있다.

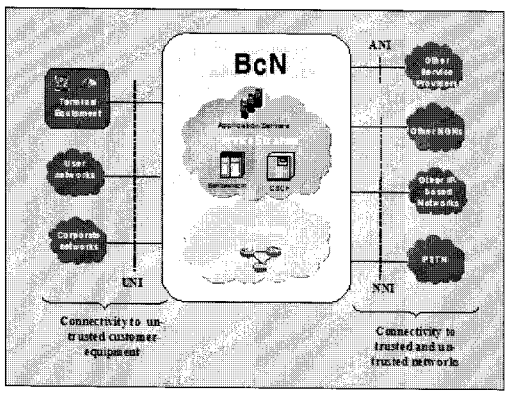

그림 2. NGN과 사용자 또는 타망과의 연결성

3-2. 다중 사업자 환경에서의 보안 모델

안전한 NGN 서비스의 제공을 위해서는 다중 사업자 도메인을 가로지르는 종단 간 통신을 위한 네트워크 기반 보안 요구 기능의 제공이 필요하다. 이는 다양한 사업자의 도메인을 가로질러 홉 단위 기반 위의 종단 간 통신의 보안을 제공하는 것이 이루어진다. (그림 7-3)은 최종 사용자 사이의 종단 간 통신을 위한 제공된 네트워크 보안 모델을 보여준다. 각각의 네트워크 세그먼트는 다중 네트워크를 가로질러 커뮤니케이션의 보안과 유용성을 용이하게 하기 위한 특정한 보안 응답도를 가지고 있다. 상호 연결된 NGN 보안은 물리적 상호연결, 피어링 모델과 사업자 정책 등에 의존한다.

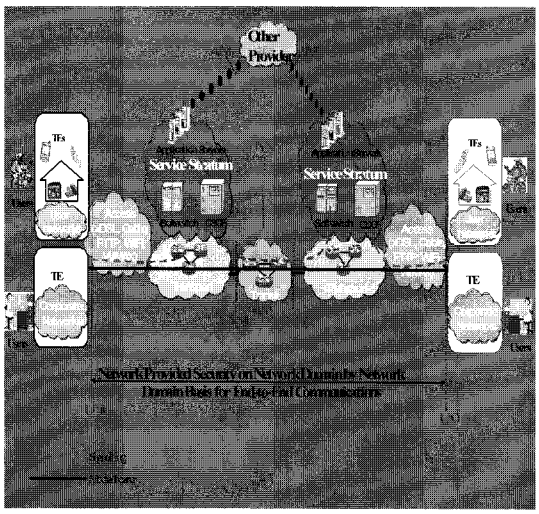

그림 3. 다중 사업자간의 보안 모델

3-3. NGN 보안 신뢰 모델

네트워크 보안은 기능 엔티티가 어떻게 묶어지는냐에 따라 달라지기 때문에, NGN 보안 구조는 네트워크 성분에 기반한다. 이러한 기능 엔티티를 네트워크 성분으로 묶는 것은 사업자에 따라 달라진다. 단일 네트워크는 (그림 4)와 같이 신뢰받은 구역, 신뢰받지만 취약한 구역, 신뢰되지 않은 구역의 3가지 보안 구역으로 정의할 수 있다. 이는 다른 장치/네트워크성분의 제어 수단, 위치와 연결성에 따라 달라진다.

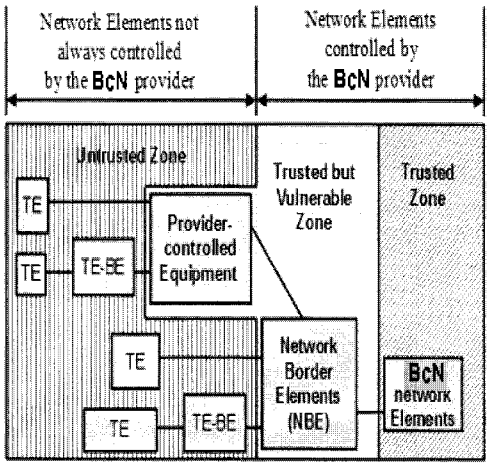

그림 4. 보안 신뢰 모델

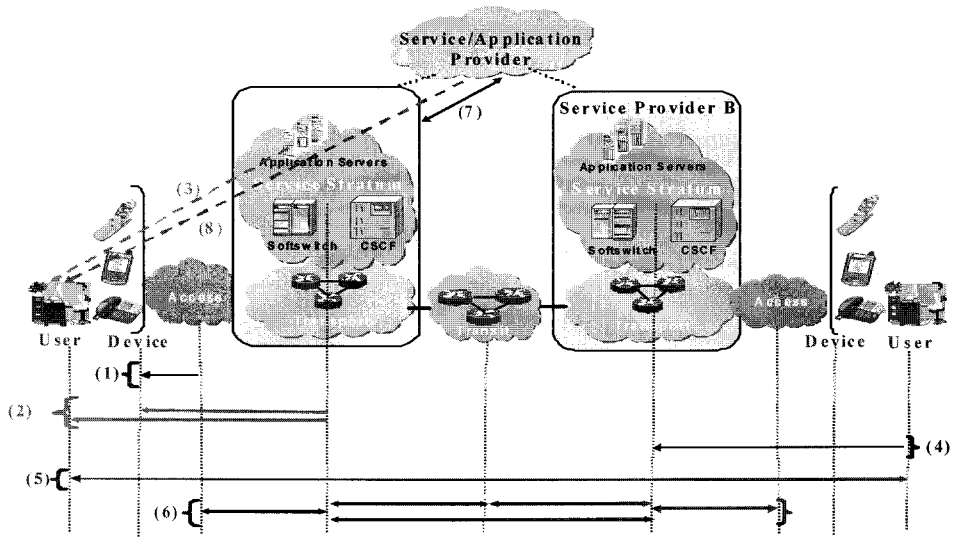

그림 5. End-to-End 참조 모델

3-4. NGN 인증 범위

안전한 BcN 서비스를 제공하기 위한 end-to-end(그림 5)와 같으며, 이를 위한 인증 범위는 아래와 같다.

① 통신망 접속을 위한 사용자의 인증과 권한부여 (예를 들면, 최종 사용자 장치, 홈 네트워크 게이트웨이 또는 사업자 게이트웨이의 네트워크에 액세스 또는 부속장치를 획득을 위한 인증과 권한부여)

② 서비스/응용 접속을 위한 사용자의 인증과 권한부여 (예를 들면, BcN 서비스/응용 액세스에 적용된 사용자, 장치 또는 결합된 사용자/장치의 인증과 권한부여)

③ 특수 서비스/응용을 위한 사용자의 인증과 권한부여 (예를 들면, ETS와 TDR 등 특수 서비스에 대한 인증과 권한부여)

④ 통신망에 대한 사용자의 인증과 권한부여(예를 들면, 연결된 BcN 네트워크 또는 서비스 제공자의 아이덴티티를 인증)

⑤ User Peer-to-Peer 사용자 인증과 권한부여(예를 들면, 수신자 및 송신자의 인증과 권한부여)

⑥ 상호적 네트워크 인증과 권한부여(예를 들면, 전송 레벨 또는 서비스/응용 레벨에 있는 NNI 인터페이스 상의 인증과 권한부여)

⑦ 서비스/응용 Provider의 인증과 권한부여

⑧ 3rd 사업자 접속을 위한 사용자의 인증과 권한부여

Ⅳ. 차세대 네트워크 AAA 서비스

4-1. NGN Id 관리 절차

그림 6 은 NG 인증을 영향을 주는 Id 기능과 서비스를 제공하기 위한 NGN 사업자의 기본 모델을 보여준다.

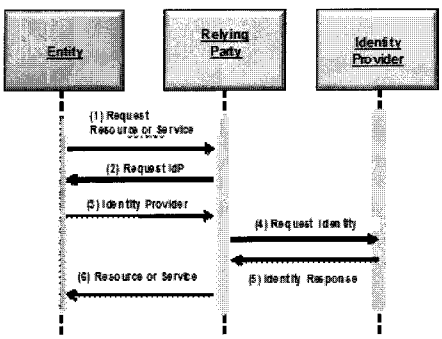

그림 6. Id 관리 정보 흐름

그림 6의 Id 참조 모델은 엔티티 (사용자), Relying Party (네트워크 또는 서비스 사업자), 신뢰와 보안 정책을 근거로 한 Id 사업자 (망 제어 또는 제3의 사업자)의 3가지 요소로 구성된다. 하이레벨의 IdM 정보 흐름은 아래와 같다.

① 엔티티는 요구되는 Id를 Relying Party에 제공하고, 자원 또는 서비스를 그 Relying Party에게 요청한다.

② Relying Party는 요청된 자원 또는 서비스를 제공하기 전에 엔티티의 Id 인증이 필요하다. 인증을 위해, Relying Party는 적절한 Id 사업자로부터 정보를 필요로 하며, 그가 결정되고 접촉시킨다. Relying Party는 엔티티가 적절한 Id 명칭을 제공하도록 요청함으로써, "Id 정보를 위한 요구"을 엔티티로 되돌린다.

③ 엔티티는 Relying Party에 적절한 IdP를 확인함으로써 이 "IdP 정보를 위한 요구"에 응답한다.

④ Relying Party는 필요에 따라 충분한 신뢰도 레벨(보증 레벨)에 엔티티의 Id를 유효화하기 위해 적절히 질문한다. 이것은 그림 6에서 "Request Identity" (인증) 단계이다.

⑤ Id 사업자는 인증을 통하여 엔티티의 Id를 확인한다. 더 높은 보증 레벨 인증이 필요한 경우 또는 다른 구현 특정적 가능성을 위해 Id 정보에 대한 Relying Party로부터 부수적인 요구가 있을 수 있다.

⑥ Id 정보로부터 엔티티의 Id를 확인한 후, Relying Party는 요청된 자원 또는 서비스를 제공한다.

4-2. NGN 사용자 인증 절차

안전한 NGN 서비스를 제공하기 위한 네트워크 및 서비스/응용 사용자 접근을 위한 인증 절차는 그림 7과 같다. 이 절차는 전송 영역과 서비스 영역 모두에서 적용된다.

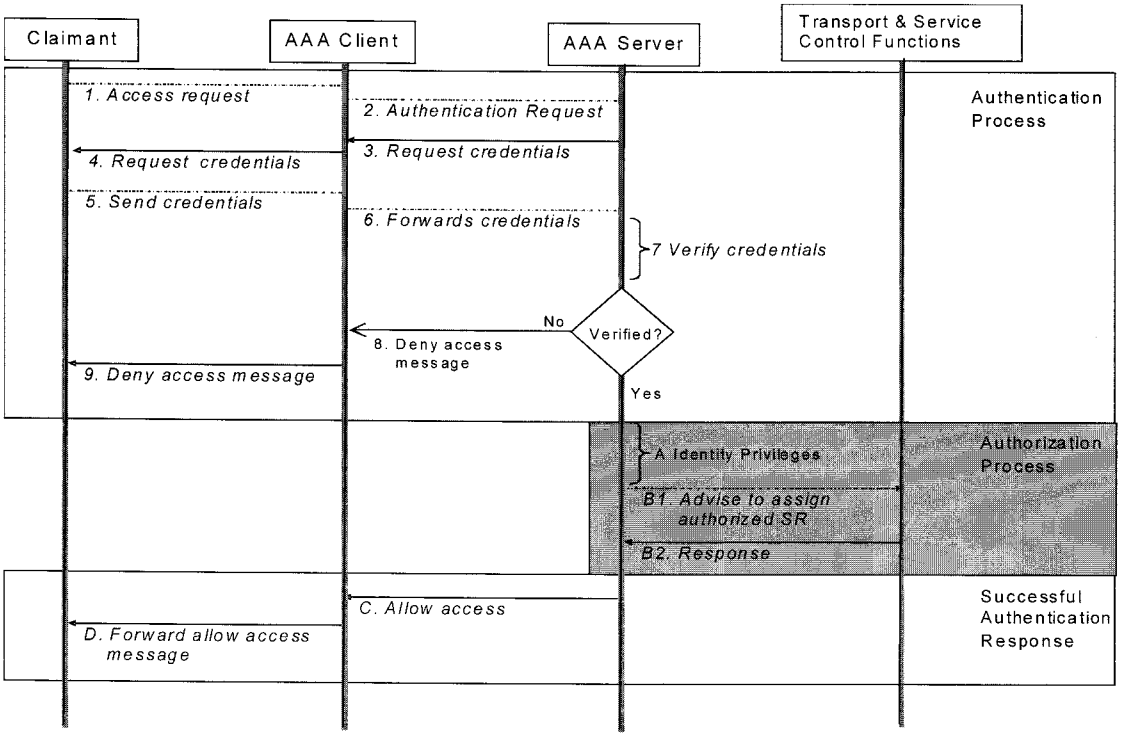

그림 7. NGN 사용자 인증 절차

(그림 7-22)의 네트워크 또는 서비스/응용 접속을 위한 사용자 인증 및 권한 부여 절차로, 하이레벨의 정보 흐름은 아래와 같다.

① 엔티티는 AAA client에서 접속을 요구
② AAA client는 AAA server에게 엔티티의 인증의 요구
③ AAA server는 AAA client에게 엔티티의 크리덴셜을 요구
④ AAA client는 엔티티에게 인증을 위해 요구되는 크리덴셜을 요구
⑤ 엔티티는 AAA client에게 요구한 크리덴셜을 송부
⑥ AAA client는 AAA server에게 엔티티의 크리덴셜 송부
⑦ AAA server는 사용자 프로파일로부터 수신된 크리덴셜을 검증
- 여기서 크리덴셜이 검증된 경우는, AAA client 또는 엔티티에게 통보하지 않고 권한 부여 과정을 수행
- 크리덴셜이 부정인 경우는, (8)과 (9) 과정 수행

⑧ AAA server는 AAA client에게 deny access msg를 송부
⑨ AAA client는 엔티티에게 deny access msg를 송부
A. AAA server는 엔티티의 서비스 또는 자원의 권한 부여 검증
B. AAA server는 엔티티의 서비스 또는 자원 접속을 위해 전송 또는 서비스 제어에게 인가된 서비스 할당을 통보
C. AAA server는 AAA client에게 allow access msg를 송부
D. AAA client는 엔티티에게 allow access msg를 송부

4-3. Security 관리 절차

안전한 NGN 서비스를 제공하기 위한 네트워크 및 서비스/응용 사용자 접근하는 순간 사용자의 log 등을 관리하는 절차는 그림 8과 같다. 이 절차 중 정보 수집 기능은 전송 영역과 서비스 영역 모두에서 지원되며, review 및 audit 기능은 망 제어 영역에서 지원된다.

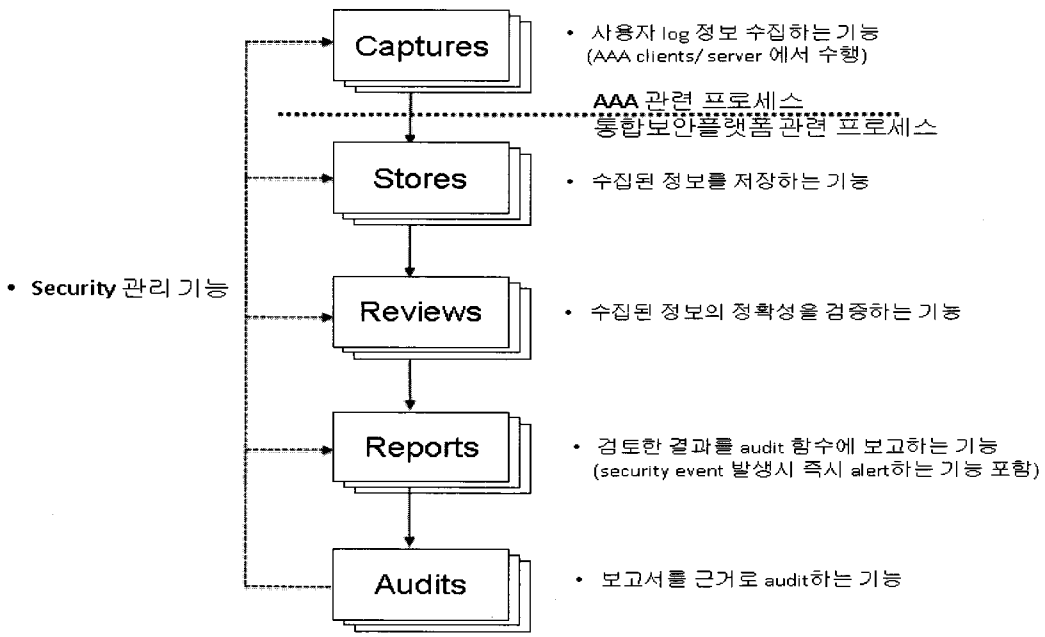

그림 8. Security 관리 절차

V. 결 론

본 논문에서는 ITU-T SG 13 Q.15 네트워크 보안 그룹에서 진행중인 차세대 네트워크 Security에 대한 표준화 동향을 기술하였다. 차세대 네트워크 보안 표준화는 주로 차세대 네트워크 보안을 위한 요구사항과 사용자 인증을 위한 모델 및 절차에 대한 권고안 작업을 진행하고 있다. 현재 표준화는 미국의 Lucent, 캐나다의 Nortel, 영국의 BT, 일본의 NIT 등이 주로 활동하고 있다.

한국의 경우 2006년 1월회의부터 네트워크 접근을 위한 AAA 기술을 표준화하는데 참여하고 있으며, 국내 BcN 기술을 차세대 네트워크 표준에 포함시켜 국제 표준화를 추진 중에 있다. 이에 국내 보안 참여 연구소, 학계, 산업계에서 NGN 보안 표준을 마련하여 차세대 네트워크 security 분야에 NGN 관련 보안 표준을 선점 할 수 있는 기반 마련이 시급하다.

참고문헌

[1] BcN 표준모델 V2.1, BcN Forum, 2006.12
[2] Y.2001: General overview of NGN, ITU-T, 2004
[3] Y.2011: General principles and general reference model for next generation networks, ITU-T, 2004
[4] Y.2012: Functional requirements and architecture of the NGN, ITU-T, 2006.9
[5] X.805: Security Architecture for Systems Providing End-to-End Communications, ITU- T, 2003
[6] Y.2701: Security Requirements for NGN Release 1, ITU-T, 2007
[7] Y.2702: NGN Authentication and Authorization Requirements, ITU-T, 2008
[8] Y.2703: The application of AAA service in NGN, ITU-T, 2008
[9] http://www.itu.int/

저자소개

오 행 석 (Haeng seok Oh)

1981년 : 한양대학교 공과대학 학사
1983년 : 한양대학교 대학원 석사
1997년 : 충북대학교 대학원 박사

1983년~현재 : 한국전자통신연구원 정보보호연구본부 융합서비스보안연구팀 책임연구원
E-mail : hsohs@etri.re.kr