BcN/NGN에서의 보안 및 액세스 인증 기술

정수환 | 최재덕
숭실대학교

요 약

개방형 망 구조의 지원으로 다양한 경로를 통하여 통신망에 대한 액세스가 쉬워지는 BcN/NGN 망에서 이를 악용한 많은 위협들이 존재하기 때문에 BcN/NGN 망에서 보안 및 인증 기술은 큰 이슈다. 본 고에서는 BcN/NGN 망에서의 보안 위협과 최근 ITU-T에서 NGN 보안 표준과 관련하여 진행중인 NGN 망에서 인증, 시그널링 데이터 보호, 미디어 데이터 보호를 위해 사용되는 보안 메커니즘들에 대해서 살펴본다. 또한 최근 ITU-T SG 13에서 개최한 NGN을 위한 디지털 아이디 워크샵에 대한 근황을 알아본다.

I. 서 론

BcN (Broadband convergence Network)과 NGN (Next Generation Network)은 용어의 명확성과, 방송융합 시점 등에서 다소 차이가 있지만, 통신 · 방송 · 인터넷이 융합된 품질 보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊어짐 없이 안전하게 광대역으로 이용할 수 있는 차세대 통합 네트워크라는 공통점을 갖는다. 또한 BcN/NGN에서는 이기종 망간 통합 및 여러 사업자간에 연동이 이루어지는 통합 네트워크이기 때문에 개별 통신망에서의 위협이 전체 통신망으로 확산될 수 있으며, 네트워크 대역폭의 증가로 전송 속도가 빨라져 악성 웜 등의 확산을 가속화 시킬 수 있는 부작용도 공통적으로 갖고 있다. 이에 유비쿼터스 사회를 앞당길 BcN/NGN 망의 발전과 함께 정보보호 문제는 간과할 수 없는 중요한 문제가 되고 있다.

국내의 BcN 기술과 대응되는 NGN 기술 표준화를 추진하고 있는 국외 표준화 그룹은 ITU-T SG13이다. 현재 NGN 보안 관련 표준 작업을 진행하는 그룹은 ITU-T SG13 Q15와 SG11의 Q7이며 각각 NGN 보안 요구사항 [6] 및 가이드라인을 [7] 발표하였고, NGN 액세스 인증 기술에 [8] 대한 표준을 다루고 있다. 현재 NGN 릴리즈 1에 대한 보안 요구사항, NGN 인증, NGN 보안 메커니즘, NGN ID 관리 및 보안에 대한 표준화 작업이 활발히 이루어지고 있다. 본 고에서는 NGN 망에서 인증과 [10] NGN 망에서 사용되는 보안 메커니즘들을 [11] 정의한 표준 문서들을 살펴본다.

본 고는 다음과 같이 구성된다. 2장에서 BcN 및 NGN 망에서 보안 위협에 대해서 알아보고, 3장에서 NGN 망에서 인증에 대해서 살펴보고, 4장에서 NGN 망에서 사용되는 보안 메커니즘들에 대해서 설명한다. 5장에서 NGN 표준화 동향으로 NGN 망에서의 디지털 아이디에 대한 표준화 동향에 대해서 살펴보고, 6장에서 결론을 맺는다.

II. BcN/NGN 망에서의 보안 위협

2.1 BcN에서의 보안 위협

BcN에서는 유 · 무선 연동, 통 · 방 융합 등이 이루어짐에 따라, 특정 접속망에서의 위협이 BcN을 통해 무선, 방송, 음성, USN까지 피해를 줄 수 있으며, BcN 환경은 개방형 어플

리케이션 인터페이스로 인해 쉽게 액세스가 가능한 점이 공격에 악용될 수 있다.

BcN 망에서는 각 계층별로 정보보호 위협을 분류할 수 있다. 서비스 계층은 Open API 기반으로 여러 응용 서비스들이 제공되게 되는데, 이러한 개방 환경에서 서비스를 제공받는 사용자들의 개인정보 유출 위협이 존재한다. 제어계층은 QoS, 이기종망 연동, 통 · 방 융합 등에 관련된 제어 기능을 수행함에 있어서 서비스 게이트웨이의 신뢰성 보장 및 관리 접근 정보의 보호 문제가 나타날 수 있다,

전달계층은 QoS를 보장하는 중요한 핵심 계층으로써, QoS에 관련된 정보의 위 · 변조 및 거짓 정보를 유포함으로써, QoS 보장을 저해할 수 있다. 접속계층은 다양한 접속 기술이 연동되고 단말기의 이동성이 보장되는 환경에서 공격의 역추적이 어려울 수 있다. 단말계층을 살펴보면, 홈기기 및 기타 다양한 단말에 통신모듈이 탑재됨으로써, 이로 인해 취약성이 대폭 증가할 수 있다.

2.2 NGN 망에서 액세스 인증 위협

ITU-T X.800과 X.805 권고안에서는 차세대 네트워크에 적용 가능한 일반적인 보안 위협을 정보와 자원의 파괴, 정보의 폐기 또는 변경, 정보와 자원의 도난/유출/손실, 정보의 노출 등으로 분류하여 정의한다. 또한 NGN에서는 추가적으로 액세스 인증에서 발생할 수 있는 보안 위협을 [8] 나타내고 있다.

• Success or Failure Indications

가입자가 네트워크에 액세스할 때 공격자는 잘못된 인증 실패 메시지를 사용하여 사용자를 속일 수 있다. 공격자는 DoS 공격을 할 수 있고 잘못된 인증 실패 메시지의 번호를 보냄으로 인증 시그널링을 망가뜨릴 수 있다.

• MITM (Man in the Middle) 공격

공격자는 실제 가입자와 실제 인증자 사이에서 고객 장비 또는 인증자에게 승인을 요구할 수 있다. MITM을 사용하는 공격자는 실제 가입자와 실제 인증자 사이에서 보안 설정 등의 관련 정보는 빼어낼 수 있고 사용자가 통신하는 모든 내용을 알 수가 있다.

• Replay 공격

공격자는 확실한 인증 메시지를 재전송함으로 인증을 실패하거나 성공하도록 할 수 있다.

• Device Identifier 공격

인증자는 사용자의 장비를 장비의 ID를 사용하여 인증한다. 인증이 성공되면, 인증자는 인증된 트래픽을 장비의 ID를 통해 제어한 이후에 사용자는 장비 ID와 패킷을 함께 전송한다. 그러나 공격자 역시 인증 작업 없이 장비 ID를 사용하여 패킷을 보낼 수 있다.

• Client Leaving the Network

사용자가 액세스 네트워크를 막 떠나려고 할 때, 사용자가 떠나기 전에 사용자는 서비스 종료의 인증자에게 알려야 한다. 만약 사용자의 장비가 통보 없이 떠났다면 공격자는 사용자인 척 할 수 있고 네트워크를 사용하거나 중간 메시지를 전송할 수 있다.

• Service theft

공격자는 네트워크 액세스에게 인증된 클라이언트인 척하여 네트워크 액세스 서비스를 가로챌 수 있다. 사용자가 성공적으로 인증이 된 후에 실행 지점은 네트워크로의 인가되지 않은 트래픽을 예방하기 위해 트래픽을 제어한다. 이러한 필터링은 IP나 MAC주소 기반이다. 만약 공격자가 패킷 안에 있는 IP와 MAC 주소를 스푸핑 한다면 공격자는 Service theft 공격을 쉽게 실행할 수 있다.

• DoS 공격

액세스 네트워크는 많은 종류의 DoS 공격에 취약하기 때문에 프로토콜은 반드시 DoS 공격을 예방하도록 설계 되어야 한다. 공격자는 많은 인증 요청을 사용하여 인증자에게 집중된 공격을 실행한다. 인증 작업 동안에 사용자 인증 정보의 상태가 유지되기 위해 인증자에게 상주된다면 공격자는 인증자 또는 인증서버의 자원을 고갈시킬 수 있다.

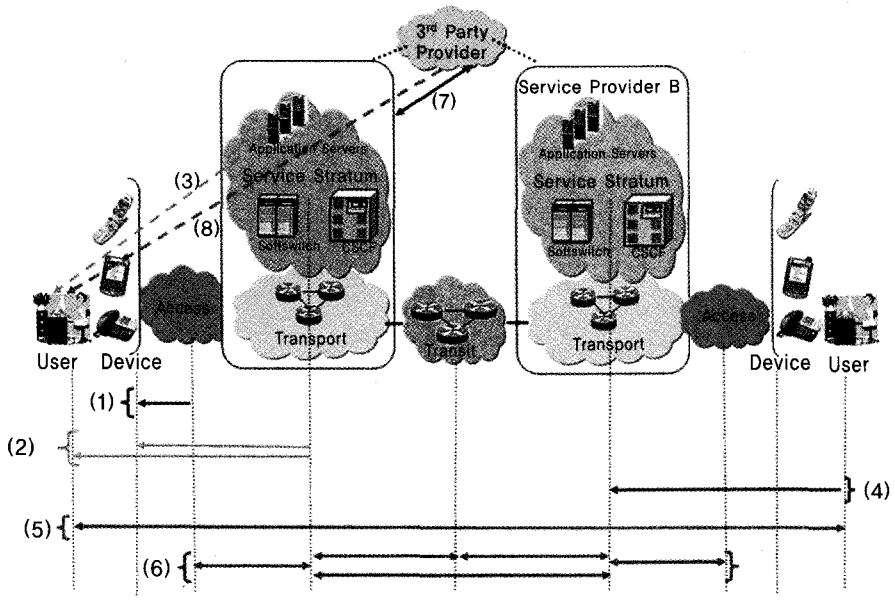
III. NGN 망에서 인증

Y.NGN Authentication 문서 [10]는 NGN 릴리즈 1과 Y.NGN-FRA [9] 버전에서 NGN 인증 및 권한 부여에 대해서 설명한다. 또한 NGN 엔티티들 간에 (User to Network (UNI), Network to Network (NNI), Application to Network (ANI)) 각 인터페이스에서 인증 및 권한 부여에 대한 요구사항도 설명한다. NGN에서는 아래와 같이 8가지 경우에 대해 양단간 인증을 제공한다. 그림 1은 NGN에서 양단간 인증 참조 모델을 보여준다. Y.NGN 인증 문서에서는 현재 ①, ② 항목에 대해서만 설명하고 있으므로, 이번 장에서는 이 두 인증 모델에 대해서 설명하도록 한다.

① 네트워크 액세스를 위한 사용자 인증 및 권한 부여 (예, 단말 - 홈 게이트웨이)
② 서비스 및 응용 액세스를 위한 사용자 인증 및 권한 부여 (예, 단말 - 서비스 제공 사업자)
③ 특정 서비스 및 응용 액세스를 위한 사용자 인증 및 권한 부여 (예, 단말 - ETS (Emergency Telecommunications Service) 서비스 제공 사업자)
④ NGN 네트워크에 대한 인증 (사용자가 네트워크에 대해서 인증 수행)
⑤ 단대단 (Peer-to-Peer) 인증 및 권한 부여 (Caller와 callee 간 인증)
⑥ 네트워크 간에 상호 인증 (예, NNI 인터페이스 간에 인증 및 권한부여)
⑦ 응용 서비스 제공 사업자와 제 3의 기관 간에 인증 및 권한 부여
⑧ 제 3의 인증 서비스 사용

3.1 네트워크 액세스를 위한 사용자 인증 및 권한 부여

네트워크 액세스 인증은 CPE (Customer Premise Equipment)와 CPE-BE (Border Element) 간에 네트워크에 액세스하려는 사용자에 대하여 아이디를 식별하고 액세스에 대한 권한을 부여함으로써 불법 사용자에 대한 네트워크 액세스를 차단한다. 단말의 네트워크 액세스 인증 및 권한 부여는 NACF (Network Attachment Control Function)의 일



(그림 1) NGN에서 양단간 인증 참조 모델

부 기능으로써 NAP (Network Access Point)가 단말의 MAC 주소, ACL (Access Control List), 사용자 프로파일 등을 사용하여 수행한다. 그림 2는 네트워크 액세스 인증 및 권한 부여를 위한 참조 모델을 보여준다. 각 구성요소에 대한 설명은 다음과 같다. 사용자 도메인은 신뢰할 수 없는 도메인 영역으로 사용자의 단말들이 위치한다.

- 레거시 CPE와 CPE-BE

레거시 CPE는 아날로그 또는 ISDN과 같은 협대역 액세스를 위한 레거시 사용자 단말이다. CPE들은 NPG (Network Provider Gateway)로부터 IP 네트워크 액세스에 대한 권한을 얻고, NPG는 CPE가 NGN 네트워크에 SIP 시그널링 및 IP 연결을 제공한다. 레거시 CPE-BE는 홈 네트워크 게이트와 같은 여러 레거시 CPE들이 접속하는 접속점이다.

- IAD (Integrated Access Device)를 포함하는 레거시 CPE와 CPE-BE

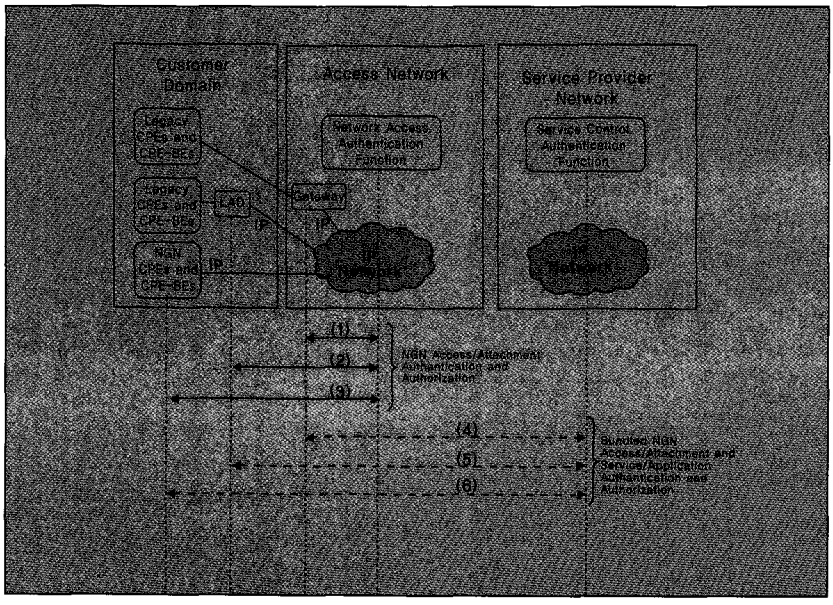
IAD와 함께하는 레거시 CPE는 xDSL 또는 케이블과 같은 광대역 액세스를 위한 레거시 사용자 단말이다. CPE들은 IAD를 통해서 네트워크 액세스 권한을 얻는다. 레거시 CPE-BE는 광대역 액세스 접속점을 지원한다.

- NGN CPE와 CPE-BE

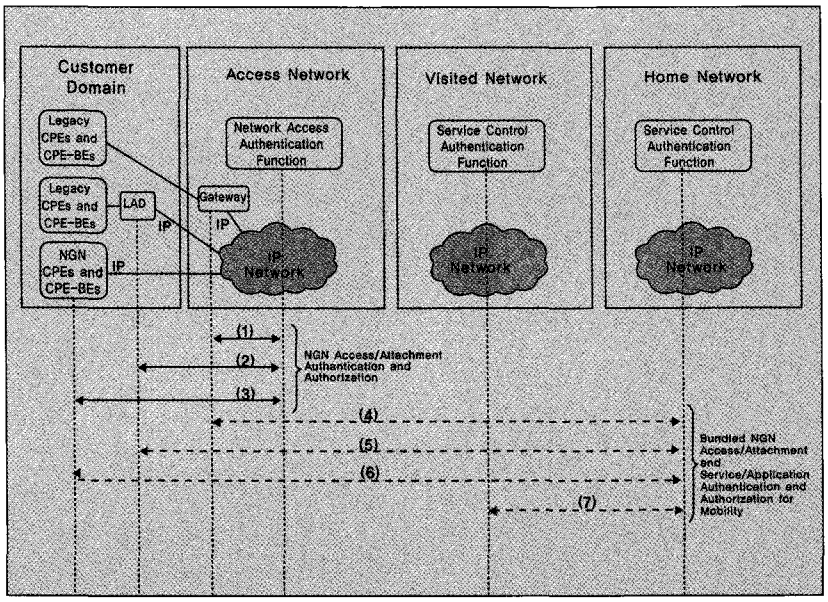
NGN CPE는 xDSL 또는 케이블이 지원되는 광대역 망에서 IP 네트워크에 직접 연결하는 사용자 단말이다. NGN CPE-BE는 IP 네트워크에 직접적으로 연결을 지원하는 접속점이다. NGN CPE와 CPE-BE의 IP 네트워크 연결은 SIP 시그널링 통신도 지원한다.

NGN Access/Attachment 인증 및 권한 부여는 ((1), (2), (3)) IP 네트워크에 액세스하려는 사용자 단말의 식별, 인증, 허가 등의 보안 서비스를 제공한다. 사용자 도메인의 각 CPE와 CPE-BE는 액세스 네트워크 도메인에 위치한 NACF에 의해서 식별, 인증 및 권한 부여 서비스를 제공 받는다. Bundled NGN Access/Attachment와 서비스 인증 및 권한 부여는 ((4), (5), (6)) NGN 서비스 사업자 인증 및 권한 부여와 함께 액세스 네트워크 사업자의 액세스 인증 서비스를 제공받는다. NGN 서비스 사업자는 각 CPE와 CPE-BE에 대해서 암시적으로 액세스 인증 및 권한을 부여한다.

(그림 3)은 이동성이 지원되는 NGN 망에서 인증 참조 모델이다. 이 참조 모델은 방문 네트워크와 홈 네트워크가 분



(그림 2) 네트워크 액세스 인증 및 권한 부여를 위한 참조 모델



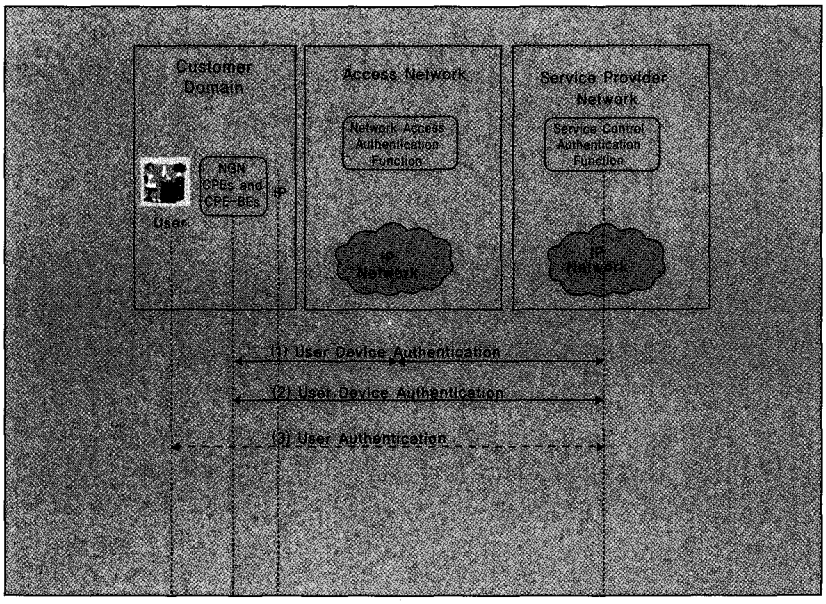
(그림 3) 방문 네트워크에서 네트워크 및 서비스 액세스 인증 및 권한 부여 참조 모델

리되어 있는 것을 제외하고 (그림 2)의 모델과 유사하다. 방문 네트워크 도메인은 다른 사업자에 의해서 운영되는 NGN 망이며, 방문 네트워크에 가입된 사용자에게 NGN 서비스를 제공한다. 마찬가지로 홈 네트워크 도메인도 홈 네트워크 사업자측에 등록된 사용자에 대해서만 서비스를 제공한다. 이 모델에서 단말이 방문 네트워크로 이동하고 홈 네트워크의 서비스를 이용하려고 할 때, 방문 네트워크에서는 단말에 대한 인증 정보를 갖고 있지 않기 때문에 먼저 홈 네트워크와 서비스 액세스 인증 과정을 수행한다. 단말은 bundled NGN Access/ Attachment와 서비스 인증 및 권한 부여 부분 ((4),(5),(6))을 수행하고, 홈 네트워크는 단말에 대해 인증이 성공적으로 이루어지면 방문 네트워크에게 단말에 대한 아이디, 인증 및 권한 검증 정보 등을 전달하여 ((7)) 단말이 방문 네트워크에서도 서비스를 이용할 수 있도록 제공한다.

3.2 서비스 액세스를 위한 사용자 인증 및 권한 부여

Y.NGN 인증 문서는 이 부분에 대해서 서비스 액세스 인증을 위한 요구사항만을 정리한 상태이다. 서비스 액세스 인증은 사용자, 사용자 단말, 사용자 및 단말 등을 식별하여 불법 사용자가 NGN 서비스를 사용하는 것을 차단한다. Y.NGN FRA NGN 구조에서 사용자 프로파일 정보를 사용하여 서비스 평층 (Service Stratum)에서 인증 및 권한 부여 기능이 제공된다. (그림 4)는 서비스 액세스 인증을 위한 참조 모델이다. (그림 4)에서 NGN 네트워크 액세스 사업자는 사용자 단말의 서비스 액세스 인증을 NGN 서비스 액세스 사업자에게 리다이렉한다 (1). NGN 서비스 사업자는 사용자 단말에 장착되어 있는 SIM 카드를 사용하여 직접 인증하거나 (2), 패스워드 등을 사용하여 사용자를 직접 인증한다 (3). 서비스 액세스 인증을 위한 일반적인 요구사항은 다음과 같다.

- NGN 서비스 사업자는 사용자의 프로파일 정보를 사용하여 단말, 사용자, 단말 및 사용자에 대해서 인증 및 권한 부여가 가능해야 한다.
- 여러 도메인 (네트워크 액세스 사업자, 방문 네트워크의 NGN 서비스 사업자, 홈 네트워크의 NGN 사업자) 간에 어디에서도 NGN 서비스를 사용자가 이용할 수 있도록 인증에 필요한 정보 교환을 위한 신뢰 관계를 맺어야 한다.
- 인증 및 권한 부여에 사용되는 아이디 정보는 허가 받지 않은 접근, 조작 등의 공격에 대해서 보호되어야 한다.



(그림 4) 서비스 액세스 인증을 위한 참조 모델

- 사용자에 대한 서비스 액세스 인증과 네트워크 액세스 인증이 함께 수행되는 것이 가능해야 한다.

IV. NGN 망에서 보안 메커니즘

Y.secMechanisms [11] 문서는 NGN 릴리즈 1 보안 요구사항을 정리한 Y.2701 문서에서 인증, 시그널링 데이터 및 미디어 데이터 보호에 사용되는 보안 메커니즘들에 대해서 기술하고 있다.

4.1 식별 및 인증 (Identification and Authentication)

• NGN 네트워크에서 인증정보 (Credential)

사용자가 NGN 서비스를 이용하기 위해서는 인증자 (예, P-CSCF, NAP)로부터 가입자 및 단말에 대한 식별 및 인증을 받아야 한다. 이러한 과정은 인증자와 CPE 간에 인증정보 (Credential)를 교환함으로써 이루어진다. NGN에서 인증정보는 X.509 인증서와 공유 비밀키 2가지로 분류된다. X.509 인증서와 공유 비밀키는 NGN 네트워크 요소들 간 또는 CPE와 인증자 간에 안전한 전달 채널을 형성하는데 사용된다. 또한 공유 비밀키는 초기 요청 메시지에 대한 응답 (SIP INVITE 또는 REGISTER 메시지 인증 과정)을 검증하는데 사용될 수도 있다.

공유 비밀키는 SAA (Service Authentication Authorization)/TAA (Transport Authentication Authorization)-FEs와 subscriber 또는 end-user가 각각 공유한다. NGN 보안 구조에서는 인증정보를 device 인증정보, subscriber 인증정보, end-user 인증정보로 분류한다. Device 인증정보 (예, 단말 시리얼 번호)는 단말 제조업체에서 생성하는 정보로 NGN 네트워크에서 단말을 식별하고 인증하는 정보이다. Subscriber 인증정보는 NGN 서비스에 가입한 후, 서비스를 이용할 수 있는 인증정보를 SIM 카드 등에 저장된 것을 말한다. Subscriber는 사람이 아닌 서비스 관련 인증정보를 SIM 카드에 저장하고, 이 SIM 카드를 사용하여 서비스를 이용할 수 있는 인증정보 자체를 말한다.

End-user 인증정보는 특정 사용자를 식별 및 인증하는 정보이다. 또는, end-user는 subscriber와 관련된 서비스를 이용하는 사람이라고 정의할 수 있다. Subscriber와 end-user

는 하나의 같은 객체로 볼 수도 있고, 하나의 subscriber에 여러 end-user로 구성될 수 있다. 예를 들어 어떤 서비스에 가입된 정보가 담겨 있는 SIM 카드를 사용하여 여러 사람들이 각각 다른 단말기에 장착하여 사용하는 경우를 말한다.

SAA/TAA-FE는 device, subscriber, end-user에 대한 각각의 인증정보들을 모두 저장 및 관리한다. 이동성이 지원되는 단말의 경우, 단말 또는 사용자의 아이디를 사용하여 외부 네트워크에 있는 인증자가 SAA/TAA-FE에 저장되어 있는 인증정보를 요청할 수 있다. 〈표 1〉은 SAA/TAA-FE에 저장되어 있는 인증정보의 한 예이다.

〈표 1〉 SAA/TAA-FE에 저장된 인증정보 예

For a subscriber certificate assigned to the John Doe family: Subscriber Account : Doe-family From headers : sip:*Doe@NGN .ngn.com Identity string : sip:Doe@NGN .ngn.com Type of credentials : subscriber End-User ID required : no	For a pre-shared key assigned to the John Doe family: Key name : JohnDoe Key : dfe56131d1958046689d8330 6477ecc From headers : sip:*Doe@NGN .ngn.com Identity string : sip:Doe@NGN .ngn.com Type of credentials : subscriber End-User ID required : no

• Subscriber 및 End-user의 식별 및 인증

SIP INVITE 메시지의 From 헤더에 subscriber에 대한 아이디가 포함된다. 그러나 이 아이디는 공격자에 의해 손쉽게 위조가 가능하므로 정당한 subscriber에 대한 식별 및 인증을 수행할 수 없다. Subscriber 식별 및 인증 기법으로 이 문서에서는 세 가지 방법을 제시하고 있다. 즉, SIP 요청 메시지의 소스 아이피 매핑, TLS/IPSec 보안 채널 사용, challenge/response 방법이다.

IP 매핑 방법은 가장 간단한 방법으로 설명하고 있고, TLS/IPSec 보안 채널을 통한 SIP 메시지 전달 방법은 X.509 인증서 기반의 방식을 제시하였다. Challenge/response 방식은 SIP 요청 메시지에 대해서 P-CSCF가 임의의 랜덤값으로 SIP 요청자에게 응답하고, SIP 요청자가 사용자 아이디와 패스워드를 사용하여 적절한 인증정보를 생성할 수 있는지 확인을 통해 식별 및 인증을 수행하는 방식이다. End-user 인증 메커니즘은 TLS/IPSec 보안 채널을 사용하는 것과 challenge/response 방식이 있다.

• Authenticator-SAA/TAA-FEs 인터페이스

NGN 네트워크에서는 사용자 및 단말에 대한 인증정보가 없는 인증자가 모든 인증정보를 저장 및 관리하는 SAA/TAA-FE에게 인증정보를 요청하여 인증 과정이 이루어진다. 그리고 대량의 인증 요청 메시지가 하나의 SAA/TAA-FE에 집중되는 부하를 분산시키기 위해서 여러 인증자들 사이에 SAA/TAA-FE가 분산되어 배치될 수도 있다. 일반적으로 SAA/TAA-FE는 AAA 서버의 역할을 수행한다.

이러한 구조에서 인증자와 SAA/TAA-FE 간 안전한 통신 프로토콜이 요구된다. RADIUS와 DIAMETER 프로토콜이 이러한 목적을 위하여 사용된다. 인증자는 RADIUS/DIAMETER 클라이언트가 되고, SAA/TAA-FE는 RADIUS/DIAMETER의 서버 역할을 수행한다. 두 노드 사이에는 상호 인증을 위하여 확장된 SIP 다이제스트 인증 기법이 사용된다.

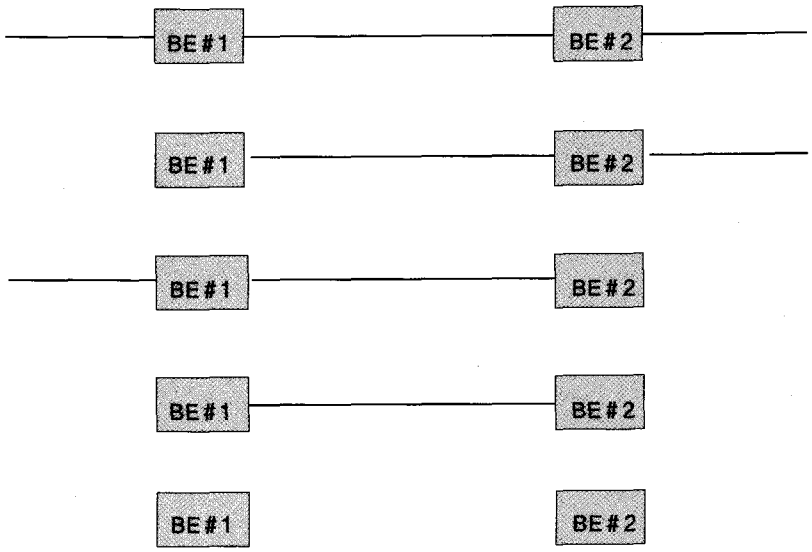
4.2 시그널링 보호

NGN 네트워크에서 시그널링 데이터에 대한 기밀성 및 무결성을 보장하기 위하여 TLS와 IPSec 보안 프로토콜이 사용된다. TLS는 SIP, COPS, TRIP, HTTP의 시그널링 데이터에 대해서 네트워크 노드들 간에 상호 인증 및 데이터에 대한 기밀성, 무결성을 제공한다.

기본 암호 알고리즘으로 TLS_RSA_WITH_AES_CBC_SHA와 TLS_DHE_RSA_WITH_AES_128_ CBC_SHA를 제공할 것을 권고하고 있다. 또한 TLS의 세션 재사용, 캐쉬, 세션 키 교환 메커니즘도 기본 TLS의 방법을 그대로 적용하고 있다. IPSec은 SNMP, RADIUS 트래픽을 보호하기 위해 사용한다. IPSec의 AH, ESP와 터널 모드 또는 트랜스포트 모드가 모두 사용 가능하다. IPSec의 키 교환 방법으로는 IKE (Internet Key Exchange)가 사용된다.

4.3 미디어 데이터 보호

미디어 데이터 암호화는 NGN에서 요구되지 않지만, 미디어 암호 사용을 요구하는 사용자들을 위하여 사용될 수 있다. 미디어 데이터 암호는 NGN 망에 경계 구성요소 BE (Border Element)들을 두어서 사용자의 요구에 따라 다양한 경우로 지원할 수 있다. 망 구성은 (그림 5)와 같이 나타난다. 그림에서 붉은 색은 단말과 BE 사이에 미디어 데이터가 암호가 된 경우이다.



(그림 5) 미디어 데이터 보호를 위한 시나리오

미디어 데이터 암호 프로토콜은 IETF에서 정의한 SRTP (Secure RTP)를 사용한다. SRTP는 AEC_CTR을 사용하여 RTP 페이로드에 대한 기밀성을 제공하고 HMAC-SHA1을 사용하여 RTP 패킷에 대한 무결성을 제공한다. SRTP에 대한 키 교환 방법은 미리 공유하거나 SIP INVITE 메시지의 SDP에 파라미터들을 사용하여 교환된다. 공유키 기반에서 BE는 SRTP 마스터키를 SAA/TAA-FE로부터 받고, 세션키를 생성하여 미디어 데이터를 보호한다. INVITE 메시지의 SDP를 사용하여 키를 교환 할 경우에는 SDP의 키 교환 파라미터의 속성에 따라 SRTP 마스터 키를 얻는다.

V. NGN 보안 표준화 동향

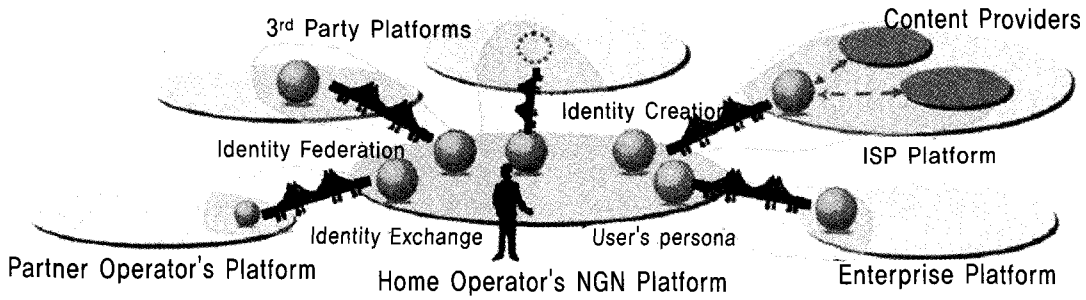
5.1 NGN에서 디지털 아이디 워크샵

ITU-T는 지난 2006년 12월 제네바에서 NGN을 위한 디지털 아이디 (Digital Identity)에 대한 워크샵을 개최하였다. 디지털 아이디란 인터넷 전자 상거래, 전자정부, 전자의료, 멀티미디어 서비스, 인터넷 쇼핑과 같이 다양한 사이버 공간에서 개인이 서비스를 이용하는데 필요한 정보를 포함하고 있는 식별자이다.

실생활에서 주민등록증, 운전 면허증, 여권, 사원증과 같이 유일하게 사용자를 구분할 수 있는 식별자라 할 수 있다. 현재 인터넷 확산과 함께 사용자가 이용하는 인터넷 서비스 수가 증가함에 따라 사용자가 기억하고 관리해야 하는 디지털 아이디 수가 증가, 개인정보 변경에 따른 분산된 사이트의 개인정보 변경시 부담 발생, 인증 수단이 미비한 아이디의 노출로 인한 신분 도용 피해 사례 급증 등과 같이 많은 문제가 발생하고 있다.

더욱이 NGN 망과 같이 통신망과 서비스의 분리를 통한 유선, 무선, 방송 융합형 서비스에서 이러한 문제는 보다 심각하게 다가올 것이다. ITU-T SG13에서는 사용자가 NGN 망에서 디지털 아이디 사용에 따른 불편함과 불연속성을 해결하기 위하여 디지털 아이디 융합에 대한 워크샵을 개최하였다.

이번 워크샵에서는 "디지털 아이디 시스템에서 요구하는 프라이버시, 식별성 및 보안 등과 같이 다양한 요구사항들을 어떻게 만족시킬 것인가?", "현재 진행되고 있는 디지털 아이디에 대한 다양한 연구 개발 과제와 표준 사이에서의



(그림 6) 디지털 아이디 컨버젼스

발생할 수 있는 차이는 무엇인가?' 에 대한 주제로 현재 진행되고 있는 연구 과제 및 표준 활동들을 소개하였다.

현재 진행되고 있는 디지털 아이디 관련 연구 과제는 Ambient Networks project, PRIME project, Daidalos project 가 있고 표준 활동은 ETSI STF 302, OASIS, ISO/IEC JTC1 SC27, Liberty Alliance에서 이루어이지고 있다.

VI. 결 론

본 고에서는 BcN/NGN 망에서의 보안 위협과 NGN 망에서 인증, 시그널링 데이터 보호, 미디어 데이터 보호를 위해 사용되는 보안 메커니즘들에 대해서 살펴보았다. 마지막으로, 최근 ITU-T SG 13에서 개최한 NGN을 위한 디지털 아이디 워크샵에 대한 근황을 알아보았다.

BcN/NGN은 현재 사용 및 제공되고 있는 네트워크와 서비스보다, 훨씬 고도화 된 차세대 네트워크 및 서비스 기술을 포함하는 새로운 개념의 네트워크로, 다양한 서비스를 쉽게 창출하고 제공할 수 있도록 개방형 구조의 통신망과 안전하고 품질 보장 및 망 관리가 용이한 통신망을 제공하는데 목적이 있다. 그러나 개방형 망 구조의 지원으로 다양한 경로를 통하여 통신망에 대한 액세스가 쉬워지고, 이를 악용한 많은 위협들이 존재하기 때문에 BcN/NGN 망에서 보안 및 인증 기술은 큰 이슈이며, 이에 따라 국내 및 국제 보안 표준 분야에서 보다 적극적인 활동이 요구된다.

또한 최근 디지털 아이디 기술이 큰 이슈가 되면서 NGN 망에서 디지털 아이디에 대한 표준화 기술 개발에 적극적으로 참여해야 한다.

참 고 문 헌

[1] 광대역통합망(BcN) 주요 장비에 대한 정보보호 가이드 (V1.0), KISA, 2006년 12월.

[2] ID 연계 기반의 인터넷 ID 관리 서비스 기술, ETRI-KISIA 1차 기술교류회 자료, ETRI, 2005년 6월.

[3] 정보통신부 BcN 구축 연동 계획 보고서 (작업문서), BcN 구축 기획반 보안망 소분과, 2005년 9월

[4] 조영섭, 진승헌, Digital Identity 관리 기술 현황 및 전망, ETRI 전자통신동향분석, 22권, 1호, 2007년 2월.

[5] BcN Forum (BcN 표준 모델 전담반), BcN 표준모델 Version 2.0, 2005년 12월.

[6] ITU-T FGNGN Document on NGN Security Requirements for Release 1, 2005.

[7] ITU-T FGNGN Document on Guidelines for NGN Security, 2005.
[8] ITU-T Draft New Baseline Document Q.NGN-nacf.sec, 2007
[9] ITU-T Draft Recommendation Y.NGN security, 2006
[10] ITU-T Draft Recommendation Y.NGN-FRA Version 0.255, 2006.
[11] ITU-T Draft Recommendation Y.NGN Authentication, November, 2006.
[12] ITU-T Draft Recommendation Y.secMechanisms, January, 2007.

약 력

정 수 환

1985년 서울대학교 전자공학과(학사)
1987년 서울대학교 전자공학과(석사)
1998년 ~ 1991년 한국통신 전임연구원
1996년 미 워싱턴 주립대(시애틀) 박사
1996년 ~ 1997년 Stellar One SW Engineer
1997년 ~ 현재 숭실대학교 정보통신전자공학부 부교수
관심분야 : 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안

최 재 덕

2002년 숭실대학교 정보통신전자공학부(학사)
2004년 숭실대학교 정보통신공학과(석사)
2004년 애드픽테크놀러지 연구원
2005년 ~ 현재 숭실대학교 정보통신공학과 (박사과정)
관심분야 : 사용자 인증, 이동인터넷 보안, SIP 보안