主題

NGN 보안

경동대학교 장 청 룡

차 례

요 약

기존의 전화망을 중심으로 하는 통신 산업은 최근의 폭발적인 유·무선 데이터 서비스 증가로 원래 데이터 서비스를 위하여 설계된 것에 다양한 데이터 응용 서비스의 하나로 전화 서비스를 수용할 수 있는 새로운 통신 인프라를 구축하려는 시도가 이루어지고 있으며 이것은 통합적으로 차세대 통신망(NGN, Next Generation Network)의 개념에서 출발하고 있다. 본 고에서는 이러한 NGN으로의 진화에 따른 고려 사항 중 보안에 대한 것에 초점을 맞추어 논의하고자 한다. 그리고, 논의의 편의상 NGN 보안을 유선계와 무선계로 나누어 소개한다.

Ⅰ. 서 론

전통적인 기존의 전화망을 중심으로 하는 통신 산업에서는 최근의 폭발적인 데이터 서비스 증가로 원래 데이터 서비스를 위하여 설계된 것에 다양한 데이터 응용 서비스의 하나로 전화 서비스를 수용할 수 있는 새로운 통신 인프라를 구축하려는 시도가 이루어지고 있으며 이것은 통합적으로 차세대 통신망(NGN, Next Generation Network)의 개념에서 출발하고 있다. 특히, 데이터 통신을 위한 인프라 구축 비용이 기존의 음성 위주의 통신망의 그것에 비하여 저렴함에 따라 차세대 통신망의 도입이 더욱 타당성을 갖게 된다. 그러나, 이를 위한 진행에는 다음과 같은 주요한 사항들이 고려되어야 한다[1,2,3]:

- 서비스 품질 : 새로운 인프라에서의 모든 전화 호와 비디오 호를 위한 적절한 자원의 배분 보장.
- 망 관리 : 망 운용 신뢰성 보장.
- 망의 진화 : 전화망에서 데이터망으로의 원만한 진행.
- 보안 : 사용요금 불법 포탈 방지, 서비스 가용성 보장, 가입자 프라이버시 보호 등.
- 경제성 : 데이터 통신량의 증가로 인한 통신 사업자의 수익 구조 변화.

본 고에서는 이러한 NGN으로의 진화에 따른 고려 사항 중 보안에 대한 것에 초점을 맞추어 논의하고자 한다.

글로벌 정보통신 시장이 꾸준히 성장함에 따라 이에 대한 보안의 중요성도 급격히 증대하고 있다. 유럽연합을 포함하는 기술 선진국에서는 공중통신망에서의 정보보호에 대한 여러 가지의 지침을 포함하여, 프라이버시와 데이터 보호에 대한 방안들을 제시하여 왔다[6]. 유럽전기통신표준기구인 ETSI(European Telecommunications Standards Institute)에서는 보안에 관한 자문 그룹을 설립하여, 공중 통신망 사업자들을 위한 보안 알고리즘의 표준화 작업을 하고 있으며 NGN 자체에 대하여는 NGN 준비 그룹(NGN-SG, NGN Starter Group)에서 구조 및 프로토콜, 종단간 품질, 서비스 플랫폼, 망관리, 법적 감청, 보안에 관한 표준화 범위를 정하여 이의 후속 작업을 진행 중에 있다[3].

본 고에서 NGN 보안에 대한 논의 이전에 차세대 통신망(NGN)의 개념과 이의 특성을 이해하기 위하여 ETSI의 NGN 준비 그룹(NGN-SG, NGN Starter Group)에서 사용하는 NGN을 소개하도록 한다. 이는 전기통신과 정보기술 산업에서 이미 시작되어 왔던 서비스 지원 인프라에서의 변화에 대하여 붙인 이름으로 통용되며 이것은 정확하게 정의된 용어라기보다는 PSTN/ISDN/GSM 2+ 단계의 후속 통신망을 표현하기 위하여 사용되는 포괄적인 것으로 이해할 수 있다[3].

이러한 NGN의 주요특징 중 하나는 서비스와 통신망을 별도로 제공되도록 하고 독립적으로 진화시킴으로써 이들을 서로 격리시킨다는 것이다. 따라서, 제안된 NGN 구조에서는 서비스를 위한 기능들과 전달을 위한 기능들을 명확히 분리시키고 있다. 이들 모두를 위한 개방형 인터페이스가 제공될 수 있으므로 NGN은 사용되는 망과 접속 유형에 상관없이 기존의 서비스와 신규 서비스를 모두 제공할 수 있게 된다.

NGN은 가능한 모든 (기지 혹은 미지의) 서비스 유형을 생성, 전개 그리고 관리할 수 있는 능력(인프라, 프로토콜 등)을 제공하여야 할 것이다. 이러한 서비스에는 모든 유형의 부호화 기법을 갖는 모든 종류의 미디어(오디오, 비디오, AV)가 이에 속한다. 이러한 서비스들은 서비스 사업자에 의한 맞춤 서비스를 강조한다. 이에 의해 대형 고객들은 자신에게 고유한 서비스를 맞춤식으로 제공받을 수 있게 된다. NGN은 또한 서비스의 생성과 제공, 관리를 지원하기 위한 서비스 관련 API(Application Programming Interface)를 가지고 있게 된다.

NGN은 기존의 단말과 'NGN 단말'을 모두 지원할 수 있다. 따라서, NGN에 접속되는 단말은 일반 아날로그 전화기, 팩스, ISDN 단말, 셀룰러 이동 단말, GPRS 단말, SIP(Session Initiation Protocol) 단말, 인터넷 전화, 디지털 세톱 박스, 케이블 모뎀 등이 이에 포함된다.

한편, 최근의 컴퓨터 범죄는 점진적으로 통신 지향적으로 되어간다. 이러한 범죄는 인터넷에만 국한되지 않으며 공중교환망 또한 해커들과 운용업체 내부 조직의 범법자들에 의해 공격의 목표로 되고 있다. 해커들은 흔히 보호되지 않은 유지보수 통신포트를 통하여 필요한 인증 정보를 얻으며 서비스 제공업체는 해커가 부정하게 얻은 서비스의 사용에 대한 요금을 대신 지불하게 될 것이다. 공중교환망에의 공격과 관련한 또 다른 예로는, 무료 통화 서비스(무료 시외전화 또는 080 서비스)의 남용이다. 그림 1은 서버나 혹은 망 구성 요소에 대한 위협 중 일부를 보여 준다. 불행히도 서비스 제공업체에 의하여 고용된 대부분의 사람들이 정직하고 믿을만하다 할지라도 모든 피고용인들을 신뢰할 수 있다고 믿는다는 것은 잘못이다. 분명히, 약간의 퍼센트는 그렇지 않을 수 있으며 일반적인 조사결과 컴퓨터 범죄의 반 정도는 해당 조직의 피고용인에 의해 범해지고 있음이 보인다[4].

프라이버시(예, 착신 번호를 포함하는 과금 데이터의 보호)는 또한 그 중요성이 증가하고 있다. 프라이

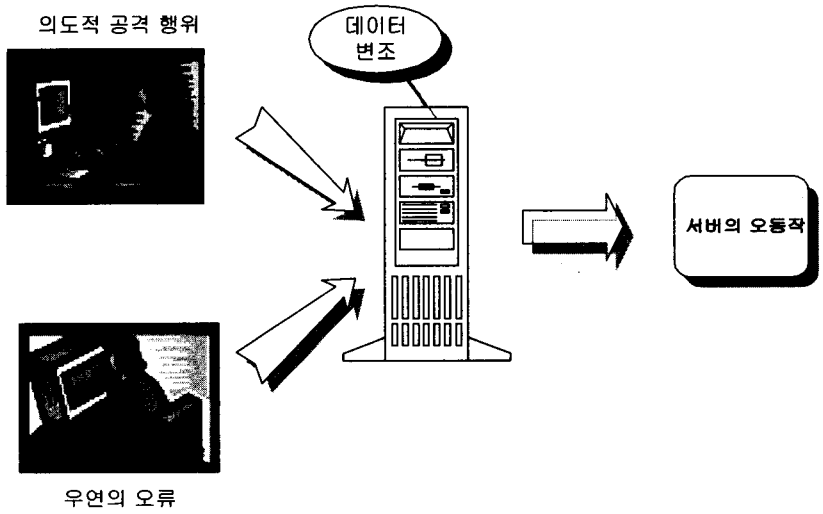


그림 1. 서버와 망 구성 요소에 대한 잠재적 위협

버시에 대한 필요성은 프라이버시와 보안에 관한 국내법과 국제적인 directive에서 잘 정리되어 있다. 공중망에서의 보안을 명확히 언급하는 유럽의 directive들이 제안되고 있다[5,6].

기술의 진보 역시 보안의 중요성에 대한 묵시적 의미를 갖는다. 지난 과거, 정보통신 장치에서 사용된 복잡한 고유의 인터페이스와 프로토콜은 쉽게 공개되거나 오용되지는 않을 것이라고 최소한 믿을 수 있었다. 이와 같은 인터페이스와 프로토콜은 제품 공급자 혹은 적어도 정보통신 집단 이외에서는 널리 알려지지는 않았기 때문이다. 이와 같은 상황은 단정적으로 더 이상 그러하지 못하다. 개방형 시스템들은 지속적으로 복잡한 인터페이스를 채택할 것이지만 이들에 많은 관심을 갖는 사람들에 의하여 잘 문서화되고 이해되고 있다.

몇 몇 신규 서비스 또한 더욱 우수한 보안기능을 필요로 한다. 이러한 서비스들은 더 이상 그들의 사용이 특정 지역에 제약을 받지 않기 때문에 위협에 더욱 노출되기도 한다. 따라서, 보안은 더 나은 경제적 또는 프라이버시의 이유로 필요하게 된다. 이들 서비스의 예로는 고품질 오디오, 화상 회의 그리고 UMTS(Universal Mobile Telecommunications System)와 3GPP(Third Generation Partnership Project)에 이해 지원되는 일반 멀티미디어 서비스가 있다. 이외에도 어떤 서비스는 관리 서비스로의 사용자/가입자 접근을 필요로 한다. 이들 사용자에게는 그들 자신만의 데이터만을 접근하도록 허용되어야 하며 이를 처리하기 위한 최소한의 기능들이 제공되어야 한다.

본 고에서는 NGN의 개념을 ETSI의 NGN-SG에서 논의된 것을 이용하고 이에 요구되는 보안을 논의의 편의상 크게 유선계와 무선계로 나누어 논의하고자 한다. 먼저 유선계 NGN 보안에 대하여는 이에 관심 있는 많은 업체중 하나인 Alcatel에서 제안하는 NGN의 보안에 대하여 소개한다. 아울러, 무선계 NGN 보안에 대하여는 유럽의 IST(Information Society Technologies) 과제의 하나인 SHAMAN 과제에서 논의되고 있는 차세대 무선통신망에서 보안에 대하여 소개하기로 한다.

II. 유선계 통신망의 NGN 진화에 따른 보안

1. 보안 요구사항

망 혹은 서비스 사업자는 위협 분석 및 위험 평가 결과에 따라 적용할 보안 조치가 무엇인가를 결정하여야 한다. 사업자가 특정 도메인를 위한 기반에 대하여 정의하는 보안 서비스, 메커니즘의 강도 등으로 구성된 집합을 "보안 정책"이라 한다. 그림 2에서는 보안 관리에 관련된 기능 블록들간의 상호 관계를 보여 준다.

위협 분석 및 위험 평가는 원칙적으로 실제 상황을 고려하여 이루어진다. 취할 보안 조치는 전체 상황에 종속되기도 한다. 따라서, 이러한 보안 정책이 주요 대형 고객들에게 어떻게 보여져야 함을 평가하고 어떤 고객이 이용 가능한 선택 사항 리스트에서 자신의 보안 정책을 적절히 맞추는 방식으로 이를 구현하는 것이 바로 사업자가 직면한 과제이다.

"정형화된 올바른" 방법으로 보안 서비스를 위한 잘 정의된 요구사항을 설정하는 과정은 약간 추상적이다. 사람들이 보안 요구사항과 서비스에 대하여 유사한 것들 중 몇 가지만을 사용하고자 하는 경향이 있다는 것은 애석한 일이다. Alcatel 사의 NGN에서는 TIPHON과제로부터의 위협 분석 방법을 업무에 적용하고 있다. 이에 대한 세부 사항은 본 고와는 거리가 있어 언급하지는 않겠으나 이것은 하향식 접근법의 좋은 예이다[7].

2. 보안 분석

보안 분석은 다음과 같은 위협들에 대하여 여러 형태의 전달서비스를 고려하여 모든 가능한 NGN 참조 구성에 대하여 적용될 수 있다:

◦ 서비스 거부(DOS: Denial of Service) : 망 구성 요소들에 대한 서비스 거부 공격은 끝임 없이 불필요한 데이터를 보내는 공세로 이루어지며 이로 인하여 여러 NGN 사용자가 사용할 망 자원들을 고갈시키게 된다. 예를 들어 음성 패킷에 의해 사용되는 통신망 경로 상에 집중적인 통화량 폭주를 야기

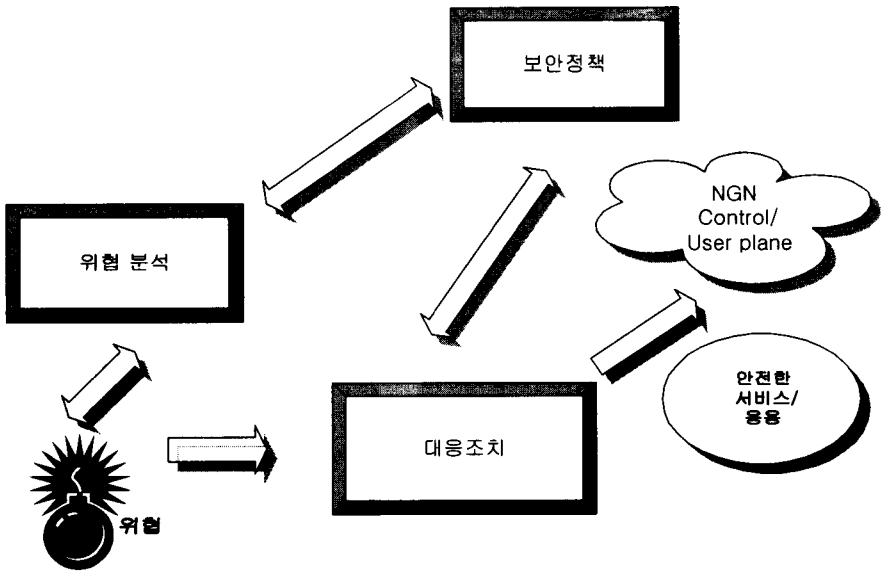


그림 2. NGN의 일반 보안 관리 모델

시킴으로써 통화를 방해하는 것이다.

◦ 정보 누출(eavesdropping) : 이것은 송신자와 수신자간의 회선을 가로챔으로서 통신내용에 대한 비밀성을 위협하게 된다. 이는 관심 있는 대화를 엿듣기 위하여 음성 패킷의 복사본을 얻음으로써 수행된다. 이러한 복사본은 통신 채널을 감시하거나 혹은 어떤 중간 라우터에 해당 패킷들을 복사하도록 명령을 내리는 방법 중 어느 하나에 의해 얻게 된다.

◦ 가장(masquerade) : 악의의 공격자는 자신의 거짓 신분을 속이기 위하여 위장을 하기도 한다. 예를 들면, 그는 특정 사용자의 ID와 패스워드를 몰래 염탐하거나, 메시지의 발신자 필드를 변조하거나 혹은 통신망 내에서 I/O 번지수를 변조시킴으로서 가짜 신분을 얻게 된다. 즉, 특정 패킷들이 마치 원래의 대화 과정에 속하는 것들처럼 보이게 하여 이들의 헤더들이 위조된 패킷들을 해당 게이트웨이로 보냄으로써 이루어진다.

◦ 비인가 접근(unauthorized access) : 망 실체에 대한 접근은 제약되어야 하며 적절한 보안 정책에 적합하여야 한다. 만약 공격자가 어떠한 통신망 실체에 비인가된 접근권을 갖는다면 앞서 언급한 서비스 거부, 정보 누출 혹은 가장과 같은 다양한 다른 공격들이 계속 될 수 있다. 비인가 접근도 역시 앞서 언급한 공격의 결과일 수도 있다. 한편, 게이트웨이와 호 처리 에이젼트들과 같은 통신 구성 장치들이 인터넷을 통하여 접근할 수 있다면, 이것은 위협이 될 수 있다. 예를 들어, 불법행위자가 통화료를 불법 포탈하기 위하여 호처리 신호 절차를 왜곡시키려고 시도할 수 있다. 또한, 해커들은 망 구성 장치들의 플랫폼 제어권을 얻기 위하여 설계 특성 혹은 프로그래밍 오류를 이용하곤 한다. 호 처리 에이젼트의 경우는 전화망으로의 공격을 개시하는 통로로 이용될 수 있어 더욱 위험하다. 대부분의 교환기는 SS7 망이 안전하다고 가정하며 이를 통하여 접수된 어떤 명령 어든지 수행한다. 호 처리 에이젼트를 제어하려는 해커는 SS7 게이트웨이를 통하여 메시지를 보낼 수 있으며 통신 인프라에 엄청난 위해를 가할 수 있다.

◦ 정보 변조(modification of information) : 이러한 경우, 의도적인 변조에 의하여 데이터는 망실되든지 혹은 쓸모 없게 된다. 이러한 행위의 한 결과로 통신망 자원에 대한 적법한 접근에 대하여도 거부당할 수 있다. 원칙적으로 사용자로 하여금 그들의 정당한 접근 권한의 범위 내에서 의도적으로 데이터를 변조시키거나 혹은 데이터베이스를 훼손시키는 것을 막는 것이 기능하지는 않다.

◦ 부인(repudiation) : 통신과정에 연루된 한 명 이상의 사용자는 NGN내의 상대측 사용자 혹은 서버/서비스와의 통신 과정에서 전체 혹은 일부에의 참여가 거부된다. 가능한 공격 방법으로는 전송 거부, 데이터 수신 거부, 데이터 접근 거부, 혹은 데이터 수정 거부가 있다. 망 운용 사업자 혹은 서비스 사업자의 관점에서, 이러한 형태의 공격은 수입의 손실, 신뢰의 실추, 결국 대형 고객의 가입 해지를 야기시키게 된다.

3. 보안 대책

보안 대책으로는 일반적으로 방지 수단 혹은 검출 수단으로 분류될 수 있다. 다음에 나열하는 것들은 NGN 보안을 위하여 전반적으로 언급된다:

- 인증(authentication);
- 디지털 서명(digital signature);
- 암호화(encryption);
- 부인봉쇄(non-repudiation);
- 접근제어(access control);
- 감사 증적(auditing Trail);
- 가상사설망(VPN : Virtual Private Network);
- 침입탐지(intrusion detection).

보안 서비스 혹은 보안 메커니즘으로의 보안 대책 활용에 대한 전반적인 해설은 참고문헌 [8]을 읽어보

기 바란다.

한편, NGN 구성 요소에서 이용되는 운영체제는 다음과 같은 기본적인 보안 대책으로 안전한 구성을 유지하여야 한다:

- 모든 비필수 기능(예, TCP/UDP 포트) 들은 비활성화 되어야 한다.
- 내부 혹은 외부 접근을 위한 원격 접근 기능은 비활성화 되어야 한다. 만약 이러한 기능이 유지보수를 위하여 필요하다면, 모든 활동이 감사될 수 있어야 한다.
- 모든 운영체제의 기능을 제어하는 서버의 콘솔은 적절한 보호조치가 있어야 한다. 모든 운용체제는 이 콘솔을 안전하게 하기 위한 특수한 기능을 갖는다.
- 전체 시스템은 이에 접속하는 전체 로그를 관리하여 감사할 수 있어야 한다; 로그 파일에 대한 주기적인 모니터링이 강력히 권고된다.

부가적으로 통신망 자체도 안전한 구성을 유지할 수 있어야 함이 강력히 권고된다. 예를 들면 망 사업자는 다음 사항을 수행하도록 제안된다;

- 디폴트 패스워드의 변경;
- 비사용 포트의 비활성화;
- 패스워드 히스토리 로그의 유지;
- 실체 인증의 활용;
- 안전한 구성 제어.

잠재적인 위협 분석과 위험 평가를 결합한 후 이에 대한 보안 대책들을 연결시킨 것이 그림 3에 보여진다.

NGN을 안전하게 운용하기 위하여 통신망 인프라와 신호 프로토콜을 보호하고 통신과정에서의 프라이버시를 보장하기 위하여 포괄적인 암호 기법의 활용이 요구된다. 더욱이, 이러한 일은 낙관적으로 보여지는 여러 가지 징조가 보이고 있다. IPsec 보안 프로토콜과 같은 적절한 보안 기술이 전개되고 있어 NGN은 기존의 전화망 보다 더욱 안전하게 운용될 것으로 기대되며 여러 가지 암호기법들이 표준화 기관으로부터 제정됨에 따라 통신의 프라이버시는 더욱

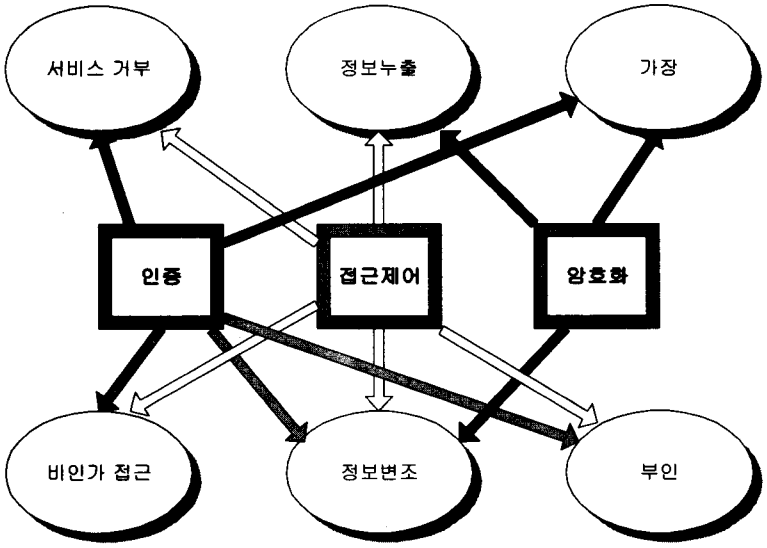


그림 3. 잠재적 위협에 대한 보안 조치

잘 보호될 것이다.

4. Alcatel의 NGN 보안 솔루션

정보통신 장비 공급 업체중 하나인 Alcatel은 NGN 보안 구조를 위한 전문가 그룹을 운영하고 있다. 3GPP에서의 인증과 같은 몇 몇 영역에서는 권고의 표준화 작업에 참여하고 있으며 이 작업은 조만간 완료될 것으로 예상된다.

VoIP(Voice over IP)의 경우에, 공유 광-동축 혼재(HFC: Hybrid Fiber-Coax) 망과 공유 IP 백본 망으로 음성과 신호 데이터를 전송하기 위함에 있어서 상세하고 완숙된 보안 규격이 PacketCable™으로 제시되었다[9].

NGN 포트폴리오에서 특별히 멀티미디어 응용의 경우, 새로운 서비스가 패킷망을 통해 제공되고 있다. 이러한 응용은 오디오, 비디오 그리고 데이터를 다양하게 결합시킨 통신을 이용하며 고정된 액세스와 이동성에 초점을 맞추고 있다. IP는 일반적으로 이들 응용에서 전달 기술로 예상된다. 물론, 원칙적으로 IP, ATM(Asynchronous Transfer Mode), MPLS(Multi Protocol Label Switching) 등과 같은 모든 형태의 패킷망은 멀티미디어 응용을 지원할 수 있다.

이들 응용에 대한 위협 분석의 결과에 의해 NGN 서버 그리고 통신망에 대한 적절한 보안 대책을 수립하여 안전하게 보호되고 있다. 통신망의 네트워크 계층과 패킷 처리 계층에서 보안을 위하여 IETF에 의해 정의된 표준인 IPsec(Internet Protocol Security)이 확실한 해결책이다. IPsec은 특별히 VPN의 구현과 다이얼-업 접속을 통한 사설망의 원격 사용자 접근에 유용하다. IPsec의 주요 장점은 개별 사용자의 통신망 구성 요소들을 변경시키지 않고도 보안 조치를 취할 수 있다는 점이다.

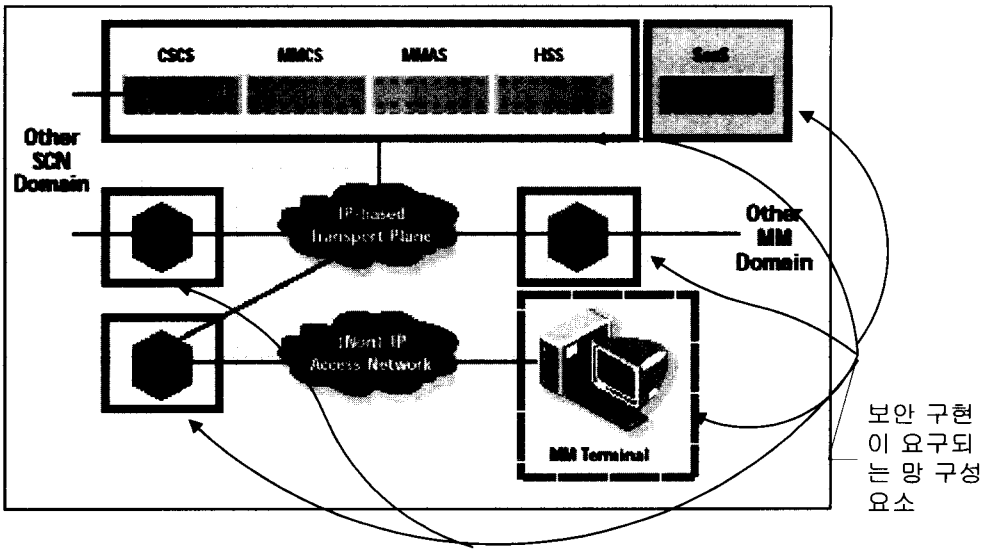
IPsec은 두 가지 선택의 보안 서비스를 제공한다: 하나는 데이터 발신자의 인증을 기본적으로 허용하는 인증 헤더(AH, Authentication Header)와 다른 하나로는 발신자의 인증과 데이터 암호화 둘 모두를 지원하는 보안 페이로드 캡슐화(ESP, Encapsulating Security Payload)이다[14]. 이와는 별도로 키 프로토콜들이 선택될 수 있으며 이와 같은 프로토콜로는 인터넷 키 교환(IKE, Internet Key Exchange)이 있다.

그림 4는 NGN 멀티미디어 서비스 구조에 있어 보안의 구현 사례를 보여 준다. NGN의 관점에서 서버와 게이트웨이들에는 소프트웨어나 혹은 선호적으로는 (보안과 성능의 관점에서) 하드웨어 플러그-인 방식중 어느 하나로 통합된 IPsec 장치로 실장되어 있다. 보안 서버(SecS, Security Server)는 보안 환경 전반을 통제하고 관리하는 기능이 요구된다. 이 보안 서버는 다음과 같은 선택적 기능을 가질 수 있다:

- VPN정책(VPN 그룹을 위한 접근 제어),
- X.509 디지털 인증서 관리,
- 관련 인증 기관과의 상호 인증서 교환,
- VPN 고객들의 원격 관리, 그리고
- 표준화된 키 생성 및 키 분배.

III. 무선계 통신망의 NGN 진화에 따른 보안

다양한 주제로 시작하는 차세대 이동통신망에 관한 보안 연구의 대상으로는 IP-기반 망으로의 진행, 다양한 접근 통신망을 통한 로밍, 사용자 중심의 서비스 및 응용에의 접근, 다양한 분산, 다기능 그리고 개별화된 장치로서의 단말이 포함된다. 이와 같은 연구 주제에서의 다양한 위협에 대한 보안이 어떻게 적용되는가에 대하여 관련 연구중 하나인 IST(Information Society Technologies) SHAMAN과제에 대하여 소개한다[10].



CSCS : Circuit Switched Call Server
HSS : Home subscriber Services
MMAS : Muitimedia Application Server
SCN : Switched-Circuit Network
GW : GateWay
MM : MultiMedia
MMCS : MultiMedia Call Server

그림 4. NGN 멀티미디어 서비스 구조에서의 보안

1. 기존의 이기종 접근 통신망과 IP-기반 통신망과의 연동

3세대 이후의 통신망 구조는 다음과 같은 몇 몇 동향으로 특징 지울 수 있는 것으로 이해할 수 있다.

◦ IP의 이용은 글로벌 접속의 중요한 요소가 된다. 이것은 기존의 유선계 핵심망에 제한되는 것이 아니라 무선 접속망까지도 연장된다. 이에 대한 프로토콜들은 IETF에서 대부분 규정된다.

◦ 이는 3세대 시스템에서의 혁신이라기 보다는 점진적인 진화에 의할 것이다.

◦ 3세대 이후의 시스템은 사용자에게 자신의 서비스를 가장 적절히 지원하도록 하는 여러 서로 다른 접근 통신망 기술을 함께 결합하여 사용하는 것으로 특징지워 진다.

이와 같은 3세대 이후의 무선 시스템에 대한 보안 구조를 규정하는 것을 목표로 하는 과제로 EU의 IST SHAMAN이 있다. 이의 구현은 그러한 무선 시스템의 적당히 상세한 규격을 이용할 만한 경우에만 개발될 수 있다. 이 과제의 첫 번째 업무중 하나는 3세대 이후의 시스템을 위한 통신망 구조들 중 참조 기준이 될만한 것을 하나 혹은 최소의 수를 선정하기 위하여 기존에 진행중인 3세대 이후의 시스템들을 평가하는 것이다. 이를 위한 유망 후보로는 다음과 같은 과제들을 거론할 수 있다[11,12,13]:

- MWIP(Mobile Wireless Internet Forum);
- Brain(IST BRAIN(MIND의 후속 과제));
- Hiper(ETSI의 HIPERLAN과 UMTS가 공동 추진).

처음 두 개의 과제들은 IETF에서 정의하는 기법의 이용에 기반을 둔 "모두 IP만으로(all-IP)"의 접근방식이며, 반면에 세 번째는 기존의 프로토콜을 이용하는 좀 단기적인 활동이다. 참조 방식의 수는 점차 줄어들 것이지만, 3세대 이후의 시스템에 대한 향후 방향이 여전히 불확실하므로 특정 해결책을 너무 일찍 선택하는 것도 그리 현명하지는 못할 것이다.

안전하게 처리될 필요가 있는 "모두 IP만으로"의 이동통신 시스템내의 필수 기능 계위에는 이동성 관리(mobility management), 서비스 품질 그리고 세션 제어가 있다.

이들 계위들은 각자가 시스템에서 다른 두 계위가 없이도 제공되므로 대단히 독립적인 것으로 보여지며 또한 이들 계위의 각각에 대한 보안 대책도 별도로 연구될 수 있다. 이와 같은 접근은 IETF에 의해 이미 취해지고 있다. 이동성 관리에 대한 보안 대책으로는 이동 IP(v4 및 v6), 계위적 이동 IP, 지역 등록 및 다양한 관련 마이크로-모빌러티 프로토콜이 있으며 이들은 각 각 고유의 보안 대책을 갖는다. 서비스 품질에 대한 보안 대책으로는 RSVP의 사용이 포함되며 이에 대하여 IETF에서는 상당히 다르게 논의한다. 세션 제어에 대한 보안 대책으로는 SIP(Session Initiation Protocol)이 있으며 이것도 IETF에서는 자체의 고유한 대책으로 논의하고 있다[14].

이러한 IETF의 접근 방식에 비하여, SHAMAN 과제에서는 이들 계위들이 서로 협력하는 시스템에 대한 논의를 목표로 한다. 따라서, 개별 계위의 보안 대책에 대한 검토는 단일 보안 구조로의 중간 단계일 뿐이다. 이는 시스템에서 고도의 복잡도와 낮은 성능을 회피하기 위하여 필요하다. 즉, 보안이란 모든 기능 계위에 걸쳐 종합화되어야 한다는 것이다. 이러한 관점에서 보안은 운용 및 유지보수와 계정관리와 같은 관리 기능과는 비교된다.

따라서, SHAMAN 과제에서는 안전한 통신망 접근 서비스에 우선 순위를 둔다. 상호 통신을 하는 사용자간의 안전한 단대단 통신, 안전한 상거래 혹은 응용 서버로부터의 오브젝트 내려 받기와 같은 여타의 보안은 차 순위의 우선 순위를 둔다.

우선 순위의 안전한 통신망 접근 서비스에는 다음과 같은 보안 서비스가 개별 혹은 함께 처리된다;

- 사용자와 접근 통신망간의 실체 인증(상호 인증),
- 무선 링크상의 트래픽 보호를 위한 암호화 및 무결성에 요구되는 세션 키 혹은 이동체 노드와 접근 통신망간의 후속 인증에 요구되는 세션 키의 생성 및 분배를 위한 키 설정,
- AAA 서버와 프로토콜에서 고려는 것과 같은 수준의 권한 부여(authorization),
- 사용자 및 신호 데이터에 대한 비밀성과 무결성,
- 글로벌 로밍,
- 통신망 서비스와 응용을 위한 통일된 접근 절차.

2. 차세대 이동 단말과 응용을 위한 보안 구조[15]

컴퓨터에서조차도 일정한 접속 장치를 부착하여 음성 전화를 할 수 있으며 강력한 기능의 무선 전화기는 휴대용 컴퓨터와 경쟁관계 있게 되며 근거리 통신망에 접속되는 단말(예, 랩톱 컴퓨터, PDA (Personal Digital Assistants), 전화기)들은 관련 통신망과 다중 접근 옵션을 갖는다.

이와 같이 컴퓨터, 전화기 그리고 통신망 접속 기기들간의 경계는 점점 모호하게 되어가서 결국, 분산 단말 그리고 개인 통신망(PAN, Personal Area Network)의 둘 모두로 일컬어지는 개인화된 통신망 기반의 통신과 전산 환경이 된다. 결국 유선계 접속 단말은 이동성의 제약으로 사용에 많은 제약을 준다. 단거리 자외선 통신인 IrDA(infrared Data Association)의 사용은 자연스러워 지지만 무선 직선거리(line-of sight)는 이의 사용을 제한한다. 향후에는 Bluetooth와 같은 단거리 무선 통신의 이용이 보편화될 것이며 대부분의 기기에 적용될 것이다.

이동 단말의 또 다른 중요한 기술적 측면으로 사용자가 몇 가지 방법으로 자신의 단말을 구성할 수 있다는 것이다. 이는 각 단말 자체에서 동적인 소프트웨어 업그레이드를 필요로 한다. 현재는 사용자가 랩톱이나 PDA와 같은 개인용 컴퓨터 기기에서 자신이 좋아하는 응용 프로그램들을 내려 받기를 할 수 있으며 이것은 이제 이동 단말에서도 역시 가능하게 되고 있다. 이외에도, 제조업체와 이동 통신 사업자는 단말 기능을 업그레이드시키고 재구성하고 싶어한다. 따라서, 차세대 단말은 동적으로 재구성할 수 있어야 하며 분산처리가 가능한 환경을 갖추게 될 것으로 예상된다.

수많은 무선 통신망의 형태는 PAN의 개념으로 정리될 수 있다. 본 고에서는, 간단한 PAN 참조 모델을 도입하여 설명하고자 하며 이는 하나 이상의 지역 통신망 서비스를 지원하는 장치, 글로벌 통신망 인터페이스를 갖는 장치 그리고 가입자 모듈 장치의 3가지 기본 구성 장치들로 구성된다.

이동 단말의 많은 핵심 기능들이 PAN상에서 접근할 수 있다는 분산 단말의 개념을 고려하기로 한다. 이것은 SIM/USIM(Subscriber Interface Module/Universal SIM) 카드에의 접근과 접속 관리 기능과 같은 핵심 단말 기능들을 포함한다. 고려할만한 적용 시나리오로서 소위 '카 시나리오(car scenario)'가 있다. 이 시나리오에서 자동차 내장 인터페이스는 고유의 가입자 모듈을 갖지는 않는다; 따라서, 이것은 가입자 모듈과 연동하는 다른 장치가 있을 경우에만 동작할 수 있다. 이와 같은 시나리오에 대한 위험 분석을 통하여 규명된 위협은 다음과 같다[15]:

- PAN 장치로 내려 받은 악성 컨텐츠.
- 어떤 비신뢰적인 PAN 장치로부터 상대 PAN 장치내의 핵심 기능으로의 접근.
- 장치 상호간 PAN 통신에서의 수동적 정보 누출.
- 정당한 PAN 장치로의 가장.

다음으로, 차세대 단말 및 응용을 위한 보안 구조를 개발하기 위하여 먼저 이러한 보안 구조가 만족시켜야 하는 보안 요구사항들을 규명하기로 한다. 간단한 PAN 참조 모델에 포함되는 새로운 역할 모델을 이용할 수 있으며 이를 위하여 다음과 같은 보안 요구사항들을 정리된다.

◦ 다양한 PAN 구성 장치들 간의 효율적인 접근 제어를 수행하고 통신 보안 정책을 정의하는 신뢰 모델의 개발.

◦ 사용자에게 알리거나 경고하는 충분한 정보를 제공하거나 혹은 특정한 통제와 구성을 방지하도록 하기 위한 통제 및 구성.

◦ 보안 구조내의 개별 PAN을 관리함에 있어서의 내부적인 통신 보안.

◦ 단말의 재구성 및 소프트웨어 업그레이드에 따른 모바일 코드의 안전한 실행.

3. 공개키 기반(PKI, Public Key Infrastructure) [16]

앞서 언급한 보안 구조를 지원하기 위하여 PKI가 요구된다. SHAMAN 과제에서는 앞서 언급한 통신망 및 차세대 단말에서의 PKI 요구사항들을 규명하고 현재의 연구결과를 기초로 다음과 같은 분야에 대한 해결방안을 모색한다:

◦ 서로 다른 PKI 환경에 대한 상호운용성: 이 문제는 어떤 사용자가 하나의 운용 환경에서 다른 운용 환경으로 이동하여 새로운 단말 성분을 선택할 경우에 발생한다. 한 도메인에서 다른 도메인으로 인증서를 번역하는 방법의 정의를 포함하여 여러 가지 상호운용성의 문제의 해결 방안을 모색 중에 있다.

◦ 보안 정책 식별자, 인증서의 자동 처리 등 권한 부여 문제: ITU-T X.509 기반의 PKI 기법은 보안 정책 식별자를 사용한다. 이것은 인증서가 발행되는 정책이 어떤 것인가를 가리키며, 인증 경로가 구축될 수 있는 방법이 어떻게 제한되는가를 포함한다. 특

히, 이동 단말의 꾸준한 증가와 많은 수의 서로 다른 CA로부터 생성되는 인증서의 처리로 정책 자체의 자동적인 처리에 대한 해결 방안의 모색이 논의되고 있다.

IV. 결언

NGN에서의 보안은 NGN을 구성하는 다양한 형태의 망 구성 요소와 단말을 중심으로 하는 유무선 서비스를 복합적으로 제공하는 통신망과 이에 접속된 단말에 대한 보안으로 귀결된다. 본 고에서는 먼저, NGN의 개념과 특성을 이해하고 이에 대한 보안의 논의를 유선계와 무선계로 나누어 소개하였다. 유선계에 대하여는 Alcatel에서 제안하는 NGN 보안에 대하여 소개하고 아울러 무선계 NGN 보안에 대하여는 유럽의 SHAMAN 과제에서 논의되고 있는 차세대 무선통신망에서 보안에 대하여 소개하였다.

최근 개최된 제 7차 GSC(Global Standards Collaboration) 회의(호주 시드니, 2001. 11)에서 NGN에 관한 주요 협력 분야로 ETSI의 NGN SG에서 제안된 표준화 범위 중 특히 보안 분야에 대하여는 한국의 TTA가 제안한 사이버 테러 등의 보안관련 이슈를 포함하여, NGN 구현을 위한 복합적인 보안 아키텍처와 보안 가이드라인 개발, NGN에 필요한 보안 프로토콜과 API 개발을 논의하기로 함에 따라 이를 위한 관련 연구와 활동이 심도 있게 추진되어야 할 것이다.

참고 문헌

[1] Christian Huitema, "Challenges of the Next Generation Networks", Keynote for Internet'99 Conference, Moscow, Oct. 25~28.

[2] T. Sweeney, "Next Generation Networks: The Future of Business", http://www.alcatel.com/newslink/0102/cover.htm, Alcatel Newslink 2nd Quarter 2001.

[3] NGN SG, "Conclusion from the NGN-SG", ETSI 38th General Assembly Meeting, Nov. 2001.

[4] B. Gamm, B. Howard, O. Paridaens, "Security Features Required in an NGN", Alcatel Telecommunications Review, pp. 129~133, 2nd Quarter 2001.

[5] 장청룡, "SEED의 활용과 표준화", SIS 2000 제 5회 정보보호심포지움, pp. 397~416., 2000년 7월.

[6] 이경석 외, 민간부문 전자상거래시 암호사용에 대한 연구, 산업자원부, 1999년 10월.

[7] ETSI, "Service Independent requirements definition: Threat Analysis (TIPHON Release 4)" ETSI Technical Report 101 771 V1.1.1, April 2001.

[8] 한국정보보호센터, 정보보호총서, 제 21장 컴퓨터네트워크 보안, pp. 537~565, 1996년 12월.

[9] Cable television Laboratory Inc., "PacketCable 1.2 Architecture Technical Report, PKT-TR-ARCH1.2-V01-001231", Nov. 2000.

[10] SHAMAN Project, http://www.ist-shaman.org

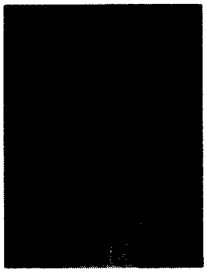
[11] MWIF,"MWIF Technical Report MTR-004", http://www.mwif.org

[12] Brain Project, http://ist-brain.org

[13] Hiper Project, http://www.etsi.org/technicalactiv/hiperlan2.htm

[14] IETF Security Area, http://www.ietf.org/html.charters/wg-dir.html#Securit

y%20Area
[15] T. Kuhn, "Interim Report - Security Architecture for Future Mobile Terminals and Applications", SHA/DOC/SAG/WP2/D03/2.0, Nov. 2001.
[16] C. Mitchell, "Initial report on PKI requirements for heterogeneous roaming and distributed terminals", SHA/DOC/RHUL/WP3/D04/1.0, Sep. 2001.



장 청 룡

1980년 2월 : 성균관대학교 전자공학과 졸업
1986년 8월 : 연세대학교 대학원 전자공학과 석사
1994년 2월 : 성균관대학교 대학원 정보공학과 박사
1979년 12월~1983년 12월 : 한국전자통신기술연구소(현, ETRI), 연구원
1984년 1월~1997년 1월 : 한국통신 연구개발본부 선임연구원
1997년 3월~현재: 경동대학교 정보보통신공학부 부교수
2001년 3월~현재 : 한국정보보호학회 학회지 편집위원장
관심분야 : 보안제품 시험, 통신망 보호, 블록암호,