主題

BcN을 위한 secure QoS 및 보안 기술 동향

대구가톨릭대학교 컴퓨터정보통신공학부 교수 전 용 희

차 례

1. 서 론

광대역 통합망(BcN: Broadband convergence Networks)이란 통신·방송·인터넷이 융합된 품질 보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊임없이 안전하게 이용할 수 있는 차세대 통합네트워크를 말한다. 이를 위하여 BcN 전달망은 서비스 품질(QoS: Quality of Service) 보장, 고도의 통신망 관리 기능과 보안(Security) 기능, IPv6 주소체계의 수용을 통하여 다양한 서비스를 쉽게 창출할 수 있는 개방형 망구조(Open API)를 도입한 통신망으로 유선·무선·방송 등의 다양한 가입자망의 특성을 통합하여 수용해야 하며, 표준 인터페이스를 통해 다양한 응용서비스의 개발 및 이용 환경을 제공할 수 있어야 한다.

인터넷에서 제공되는 전통적인 "최선(best-effort)" 서비스는 네트워크 트래픽의 상세하고 일관성 있는 수준의 QoS를 지원하기 위하여 설계되지 않았다[13]. 분산 멀티미디어, IP 전화 및 비디오 컨퍼런싱 같은 현대의 네트워크 애플리케이션들은 종단간 지연, 대역폭 및 패킷 손실률 같은 QoS 파라미터에 매우 민감하다. 이러한 새로운 애플리케이션들을 위한 서비스 요구사항을 지원하기 위하여 다른 수준의 네트워크 서비스 보장을 제공하기 위한 프레임워크 및 프로토콜들이 제안되었다. IETF에서는 새로운 프레임워크/프로토콜들이 개발되었거나 표준화가 되고 있다. 이들 중에는 ReSerVation setup Protocol(RSVP), Differentiated Services(DiffServ), 그리고 Multiple Protocol Label Switching (MPLS) 등이 있다[3,5,9].

이러한 새로운 서비스가 더욱 안전하고, 융통성 있고 예측 가능할 것으로 기대하지만, 다른 한편으론 이러한 새로운 네트워크 서비스가 서비스 거부(DoS: Denial of Service) 공격을 포함하

여 네트워크 공격을 위한 새로운 목표가 될 수 있다[4]. 그러나 아직 국내에서 BcN을 위한 secure QoS(SQoS) 및 보안을 위한 참고문헌을 쉽게 찾을 수 없는 실정이다.

BcN 구축 기본계획에서, 보안이란 정보통신망 기능의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 제반 위협과 부작용 등의 정보화 역기능에 대한 대응을 의미한다[1]. 본고에서는 BcN QoS 구조에서 적용될 수 있는 보안 메커니즘들을 살펴보고 이에 대하여 기술하고자 한다.

2. BcN 보안 특징

2.1 개 요

BcN과 같은 QoS aware 통신 시스템에서, 사용자는 각각 다른 신뢰성, 예측성과 효율성 정도를 가지고 있는 여러 가지 서비스 클래스 중에서 선택할 수 있다. 그러나 현재까지 보안은 QoS 구조에서 하나의 파라미터로 인정되지 않았으며 보안-관련 서비스 클래스가 정의되지 않았다. 이것은 종단 사용자가 보안 레벨 구성을 할 수 있는 기회가 없음을 의미한다[12].

QoS 구조에서 보안을 파라미터로 인정하지 않은 이유 중의 하나는 보안을 정량화하기가 어렵다는 것이다. 게다가 보안은 본질적으로 단일 차원이 아닌 많은 속성들, 즉, 기밀성(confidentiality), 무결성(integrity), 가용성(availability)(CIA)으로 구성되어 있다는 점이다. 그러나 이 세 개의 속성들은 하부 시스템이나 통신 채널들의 다른, 많은 경우 모순된 요구사항을 기술한다. 예를 들어 높은 보안 요구사항을 가진 두 사용자가 각기 다른 요구를 가질 수 있다는 것이다. 한 명은 높은 수준의 기밀성을 요구하는 반면에 다른 한명은 높은 수준의 무결성을 요구할 수 있다[12].

2.2 보안 요구사항

BcN에서는 다음과 같은 높은 수준의 보안이 요구된다[7]:

- 고객/가입자는 네트워크와 정확한 요금청구(billing)와 함께 제공되는 서비스에 신뢰를 가져야 한다. 게다가, 높은 서비스 가용성, 공정 경쟁과 비밀성의 보호를 요구한다.
- 네트워크 운용자, 서비스 제공자 및 액세스 제공자 모두가 운용과 비즈니스를 보호하고 고객과 공중에 대한 책무를 충족하기 위하여 보안을 필요로 한다.
- 규제 기관이 서비스 가용성, 공정 경쟁 및 비밀성을 보증하기 위하여 법안을 만들어 보안을 요구하고 시행하도록 한다.

국내에서도 대통령령으로 '정보통신망 이용 촉진 및 정보보호에 관한 법률 시행령'이 제정되어 시행되고 있지만, 증가하고 있는 보안 위협과 위험으로 추가적인 보안 요구사항에 대한 필요성이 증대되고 있다. 네트워크 혹은 서비스 제공자는 위협 분석과 위험 평가의 결과를 근거로, 어떤 보안 대책을 수립할 것인지를 결정해야 한다. 어떤 도메인에 대하여 이를 기초로 운용자가 정의하는 보안 서비스의 집합, 메커니즘의 강도를 '보안 정책'이라 한다. 보안 대책은 상황에 의존하여 취해져야 한다. 형식적인 정확한 방법으로 잘 정의된 보안 요구사항을 확립하는 과정은 다소 추상적이다. Alcatel NGN에서는 TIPHON[11]의 위협 분석이 지침서로 사용되었다[7]. 일반적인 보안 요구사항은 다음과 같다:

- 계정성(accountability)
- 신원 검정

• 인증

2.3 위협 분석

다른 형태의 전송 구조를 고려하여, 광대역 통합망에서 발생할 수 있는 주요한 위협의 형태로는 다음과 같은 것이 있다[7].

- 해킹 혹은 침입 공격 : 침입자가 어떤 지역이나 자원의 집합에 불법적인 접근을 획득한다.
- 바이러스 및 웜 : 네트워크 상에 확산되어 정보를 파괴하고 변조하며 전파된다.
- 서비스 거부(Denial of Service: DoS) : 다른 사용자에게 네트워크 자원이 이용가능하지 못하도록 데이터로 네트워크를 범람시킨다.
- 도청 : 송신자와 수신자 사이의 정보를 가로채어 비밀성을 위협한다.
- 위장 공격 : 신원을 위장하여 자원에 대한 접근을 획득한다.
- 재생 공격 : 패킷이나, 패킷 스트림을 시간이 지난 후에 재전송한다.
- 비인가 접근 : 비인가 접근으로 DoS, 도청 혹은 위장 공격이 발생할 수 있고, 위에서 언급한 위협의 결과로서 발생할 수도 있다.
- 정보 변조 : 패킷 변조나, 데이터 조작, 데이터베이스 파괴 등의 공격을 말한다.
- 송수신 부인(repudiation) : 통신에 포함된 사용자가 다른 사용자와의 통신을 일부 혹은 전부를 부정할 수 있다.

2.4 대응책

대응책은 일반적으로 예방적(preventive)과 탐지적(detective)으로 분류할 수 있다. 상기 위협에 대처할 수 있는 일반적인 대응책은 다음과 같다[7]:

- 인증(authentication)
- 디지털 서명
- 접근 제어
- 가상사설망(VPN)
- 암호화
- 침입탐지
- 감사(auditing) 및 기록(logging)
- 부인방지 대책

3. QoS 구조에서의 보안

3.1 개요

전통적인 보안 해석은 두 가지의 가능한 상태 혹은 값 즉, 안전한가(secure) 아니면 안전하지 않은가(insecure)를 가지고 있다. 그러나 이 이진(binary) 모델로는 불충분하다. 대신에 보안 혹은 그것의 속성들은 하나의 전체 범위의 값을 가지는 척도(metric)로 간주되어야 한다[12]. 그러므로 QoS 구조에 포함될 다른 보안 측면에 대한 정량적인 값에 이르기 위한 방법을 정의하여야 한다. [12]에서는 직접적인 척도 대신에 어떤 보안 속성에 대한 근사화로 사용될 수 있는 간접적인 척도를 시도하고 있다. 소프트웨어 공학 분야에서 선택된 간접 척도의 예로 Albrechts 함수점(function point)이 있다[2]. Albrechts 모델은 요구사항 사양서에서 소위 함수 점의 수를 식별함으로써 코드 크기를 평가하기 위하여 사용되는 간접적인 척도이다.

Irvine [8]등은 "변형 보안"(variant security)이라고 하는 개념을 제안하였다. 그들은 보안 메커니즘과 서비스가 보안 범위(security range)를 가지는 것으로 간주하며 그 범위는 적어도 이진(binary)이라는 가정을 하고 있다. 더구나 그들은 여러 가지의 측정 가능한 보안 변수들을 식별하였으며, 이것들이 보안 속성을 간접적으로 정량화하기 위하여 부분적으로 사용될 수 있다. 대부

분 기밀성에 대한 보안 변수들에 대하여 조사하였으며, 몇 가지 예는 아래와 같다:

- 암호의 형태(대칭 혹은 비대칭)
- 키와 블록 길이
- 암호화 라운드 수

BcN QoS 구조의 아이디어는 사용자의 필요에 따라서 자신의 품질 레벨을 결정하도록 하자는 것이다. 이와 비슷하게 보안에서도, 사용자에게 이용 가능하고 구성될 수 있는 속성을 정의하기 위하여 "보안 파라미터"라는 용어를 사용할 수 있다. 보안 파라미터는 보안 변수와 같을 수도 있고 혹은 두개 이상의 결합일 수도 있다.

보안 파라미터에 대한 스케일은 절대적 스케일, 비율(ratio) 스케일, 순서(ordinal) 스케일일 수 있다. 실제 상황에서 "~보다 더 안전한" 관계가 충분할 수 있다[12]. 이와 같은 암호에 대한 한 가지 예는 다음과 같다:

$$\text{평문} \leq \text{DES} \leq \text{AES}$$

이 관계의 해석은 DES(Data Encryption Standard) 암호법으로 인코드 된 메시지는 해당 평문 메시지보다 해독하기 어렵지만, AES(Advanced Encryption Standard)보다는 쉽다는 것이다.

사용자가 통신 세션을 시작하기 전에 보안 파라미터에 값을 할당할 것이다. 편리상의 이유로, 어떤 형태의 QoS 프로파일이 이용가능하며, 사용자나 역할에 대하여 보안 파라미터의 표준 혹은 기본 값들을 포함하게 된다. 게다가 이 스킴이 실제로 사용가능하기 위해서는 구성할 수 있는 파라미터가 사용자에 의하여 이해될 수 있어야 한다. 또한 사용자가 파라미터를 쉽게 변경할 수 있는 것도 중요하다. 보안 파라미터에서의 다른 문제점은 세션 동안, 특별히 이동 컴퓨팅에서 변할 수 있다는 사실이다. 로밍이 발생할 때, 보안 요구사항이 달라질 수 있다.

3.2 RSVP 보안[13]

3.2.1 QoS와 RSVP

본 절에서는 RSVP 보안을 기술하기 위하여 필요한 RSVP에서의 QoS 메커니즘에 대하여 간략히 알아본다. RSVP 프레임워크에서, 서비스 송신자는 서비스 수신자(들)에게 주기적으로 특별한 path finding 메시지를 내보낸다. 이 PATH 메시지와 데이터 패킷 흐름이 동일한 라우팅 경로를 따라 수신자(들)에게 전달된다. PATH 메시지는 라우팅 경로를 발견할 뿐만 아니라 경로를 따라 QoS 정보를 수집한다. 예를 들어, 송신자의 Tspec 객체 (Tspec(PATH))는 트래픽 특성을 기술하며, 반면 Adspec 객체 (Adspec(PATH))는 라우팅 경로를 위하여 이용 가능한 최소 자원 레벨을 나타낸다. 수신자는 송신자를 향하여 역 라우팅 경로를 따라 예약 메시지 RESV를 주기적으로 전송한다. RESV 메시지 내의 Flowspec 객체 (Flow-spec(RESV))는 요구되는 QoS를 기술하며, Filterspec 객체 (Filter_spec(RESV))는 세션 사양서와 함께, Flow_spec(RESV)에 의하여 정의된 QoS를 받기위하여 데이터 패킷의 집합인 "flow"를 정의한다.

3.2.2 QoS 공격 목표

QoS 공격에 대한 목표는 다음과 같다:

- QoS 서비스 요구 거부: 공격자가 예약 메시지의 전부 혹은 일부를 가로채거나 탈락시켜 QoS 예약 및 채널 설정이 지속적인 방법으로 실패하거나 악의적으로 지연될 수 있다.
- 불필요한/suboptimal 자원 예약: 공격자가 특별한 사용자의 원래 예약 요구와 많이 다

른 자원을 예약하도록 할 수 있다.

- 네트워크 이용 저하: 네트워크 시스템이 QoS 요구사항의 한 집합을 지원할 수 있을 만큼 충분한 자원을 가지고 있더라도, 네트워크가 작은 부분집합을 단지 지원하도록 공격자가 예약 프로토콜을 간섭할 수 있다.
- 예약된 QoS 저하: 어떤 경로를 따라 자원이 성공적으로 예약되고 유지된다고 하드라도, 공격자가 예약된 자원을 비합법적으로 사용할 수 있다. 예약된 자원을 훔침으로써 QoS 저하가 발생할 수 있다.

[13]에서는 RSVP에서 세 가지 종류의 공격자를 정의하고 있다: $Insider_{RSVP}$, $Outsider_{OnPATH}$, $Outsider_{Other}$. $Insider_{RSVP}$는 송신자와 수신자 사이의 예약 경로상의 RSVP-실행 라우터이다. 네트워크 시스템이 강한 인증 및 접근 제어 스킴하에서 보호된다고 하드라도, RSVP 메시지 교환을 참가하는 것이 신뢰된다. $Outsider_{OnPATH}$는 예약 경로 상의 RSVP-비실행 라우터이다. RSVP 운영에 참가하는 것이 신뢰되지 않기 때문에, 그것은 RSVP 메시지를 단지 차단하고, 지연시키거나, 변경하거나, 탈락 시킬 수 있다. 가장 약한 형태의 공격자가 $Outsider_{Other}$이다. 이것들은 예약 경로 상에 있지 않은 라우터나 종단 호스트들이다. 이 세 가지 클래스 중에서 공격력의 등위는 전개되는 보호 스킴에 관계없이 다음과 같이 분류하고 있다[13]: $Insider_{RSVP} \geq Outsider_{OnPATH} \geq Outsider_{Other}$

3.2.3 공격 예제

$Insider_{RSVP}$ 라우터가 입력 PATH 메시지 내의 Tspec(PATH)를 조용히 변조할 수 있다. 그러면 거짓 Tspec(PATH) 정보로 인하여 수신자가 예약에서 틀린 결정을 내릴 수가 있다. 이 경우 1)과 2)의 두 가지의 공격 시나리오가 가능하며, 모든 경우에 대하여 이용 가능한 자원이 충분히 있음에도 수신자가 받아야 할 수준에서 QoS를 보장 받을 수 없게 된다.

1) 예제 1

만약 Tspec(PATH)이 낮은 값으로 변경된다면, 수신자가 받을 QoS가 저하된다.

2) 예제 2

만약 공격자가 Tspec(PATH)에 대하여 높은 운영을 수행한다면, 수신자가 자신의 지역 정책에 의하여, 서비스가 더욱 비싸게 보이기 때문에 자원을 예약하지 않기로 결정할 수 있게 된다.

3) 예제 3

적극적인 공격자는 수신자가 더욱 많은 불필요한 예약을 하도록 속이기 위하여 Tspec(PATH)와 Rspec(RESV) 객체 둘 다 변조할 수 있다. $Outsider_{OnPATH}$ 또한 동일한 손해를 끼치는 같은 공격을 수행할 수 있다.

3) 예제 4

RSVP-실행 라우터가 Adspec(PATH)의 값을 변조할 수 있다. 이렇게 되면 다운스트림 상의 모든 RSVP-실행 라우터가 Adspec(PATH)를 틀리게 갱신하게 된다. 결과적으로 수신자가 더 낮거나 더 높은 수준의 QoS를 예약하게 된다.

4) 예제 5

RESV 메시지 내의 파라미터가 악의적으로 변조될 수 있다. 이 파라미터들은 멀티캐스트의 경우에서 합성이 필요한 경우가 아니면 수정되지 않는 것으로 가정된다. 악의적인 RSVP-실행 라우터가 이 파라미터들을 증가하거나 감소시켜 상위 스트림 상의 RSVP 라우터들이 불필요한 예약을 하거나 수신자에게 QoS 저하를 가져오게 된다.

5) 예제 6

TearDown(RESV) 메시지는 예약 상태가 시간이 초과한 수신자나 어떤 노드에 의하여 명시적으로 개시된다. 이 메시지를 수신하면 매치되는 예약 상태를 제거한다. TearDown(RESV) 메시지 공격은 많은 사용자가 네트워크 상의 제한된 자원을 경쟁할 때 악의적인 공격자에 의하여 사용될 수 있다.

3.2.4 대응 방법

네트워크 QoS를 지원하기 위한 RSVP 프로토콜은 위의 공격 예제에서와 같이 취약성을 가지고 있다. 이런 모든 공격은 $Insider_{RSVP}$나 $Outsider_{OnPATH}$에 의하여 쉽게 수행될 수 있으며 네트워크 QoS 제공에 심각한 손해를 끼칠 수 있다. IETF/RSVP의 보안 솔루션인 홉별 인증은 $Outsider_{OnPATH}$를 방지하는 데만 유용하며, 어떤 $Insider_{RSVP}$ 공격을 다룰 수 없다. $Insider_{RSVP}$ 공격을 다루기 위하여 [13]에서는 선택적 디지털 서명 및 충돌 탐지(SDS/CD: Selective Digital Signature and Conflict Detection)를 제안하고 있다. 기본적인 아이디어는 목표 RSVP 객체들을 두 개의 다른 그룹, constant 혹은 mutable로 분할하는 것이다. RSVP 메시지의 고정(constant) 부분에 대하여는, 목표 객체의 소스나 개시자가 자신의 개인키로 객체를 디지털 서명을 한다. 이렇게 함으로써 서명된 객체를 손상시키기 위한 $Insider_{RSVP}$를 방지한다.

RSVP 메시지의 변하는(mutable) 부분에 대하여는, 서명을 할 수가 없다. 그러나 메시지가 목적지에 도착 한 후에는 변하지 않는다. 즉, 변하는 RSVP 객체는 RSVP 운영의 "history"가 된 후 "constant"로 된다. 일단 constant로 되면, 수신된 값을 commit하기 위하여 객체를 디지털로 서명할 수 있다. 이제 서명된 히스토리가 역 경로를 따라 전송되며, 경로 상의 모든 라우터는 그 히스토리가 자신의 지역 관측과 일치하는지를 조사하게 된다.

3.3 DiffServ 보안[10]

3.3.1 신뢰(trust) 영역

DiffServ 네트워크에서는 DiffServ의 정확한 운영을 위하여 여러 개의 기본적인 신뢰 영역이 존재한다.

1) **에지 라우터와 소스 사이의 신뢰** : 패킷들은 에지 라우터에서 소스별 기준으로 감시(police)된다. 패킷들은 소스와 에지 라우터 사이에서 서비스 레벨 협약(SLA: Service Level Agreement)에 따라서 마크된다. SLA는 트래픽의 양과 트래픽의 버스티니스에 관련하여 각 서비스 클래스에 대한 제한을 정하기 위하여 에지 라우터와 소스 사이에 존재한다. SLA를 위반하는 트래픽에 대하여, 위반 패킷은 더 낮은 서비스 클래스로 강등되든지 아니면 탈락(drop)된다. 트래픽을 정확하게 감시하기 위하여, 소스의 SLA에 대한 매칭이 정확하게 수행된다고 에지 라우터는 신뢰한다.

2) **코어와 에지 라우터 사이의 신뢰** : DiffServ에서는 패킷의 PHB(Per-Hop Behavior)에 따라 패킷의 고속 라우팅을 위하여 코어 라우터를 단순화하는 것이 주요 목표이다. 따라서 코어 라우터는 패킷이 정확하게 마크(mark)되고 또한 적절하게 감시되었다는 것을 코어 라우터가 신뢰할 만큼 에지 라우터와 신뢰 수준을 가진다.

3) **SLA 무결성의 신뢰** : EF(Expedited Forwarding)와 AF(Assured Forwarding) 같은 여러 가지의 서비스들이 정확하게 수행되기 위하여 SLA 무결성에 의존한다. 만일 어떤 클래스가

과도한 트래픽으로 과부하 된다면, 낮은 클래스에 대한 성능 혹은 높은 우선 클래스의 성능 까지도 감소될 수 있다. 따라서 더 엄격한 QoS 클래스의 성능 저하를 야기하도록 네트워크 자원이 과도하게 할당되지 않도록 에지 라우터들 사이의 SLA 무결성과 함께 신뢰 수준이 존재한다.

3.3.2 잠재적인 보안 관심사

1) 자원 절도: DiffServ에서 자원의 절도가 여러 가지 형태로 발생할 수 있다. 이것은 네트워크 대역폭 절도나 패킷 PHB의 불법적인 상승을 포함하기 위하여 확장될 수 있다. 대역폭 절도는 에지와 코어 라우터 레벨 모두에서 발생할 수 있다. 에지 레벨에서 만약 패킷이 자신의 소스를 성공적으로 속일 수 있다면, 패킷은 실제 소스의 SLA 할당 대역폭의 일부를 훔치게 될 것이다. 만약 에지 라우터가 SLA 이상으로 트래픽을 전송하거나 에지 라우터를 우회한 트래픽이 코어에 직접 전송된다면, 코어 라우터 레벨에서의 대역폭 절도가 발생할 수 있다.

두 번째 형태의 절도인 패킷 PHB의 불법적인 상승은 에지와 코어 라우터 모두에서 발생할 수 있다. 에지 라우터에서, 만약 패킷이 부정확하게 감시되거나 전혀 감시되지 않으면 불법적인 상승이 발생할 수 있다. 코어 라우터에서, 정확한 PHB 행위가 실행되지 않은 경우 발생한다.

2) 서비스 거부:

DiffServ 상황에서 DoS는 네트워크 상의 완전한 자원의 절도를 나타낸다. DoS 공격은 DiffServ에 대한 주요한 보안 위협이다.

먼저, DoS 공격이 출력 트래픽과 함께 에지 라우터에서 발생할 수 있다. 플로우의 감시가 DoS 공격을 일으키기 위하여 이용될 수 있는 공격점을 나타낸다. 에지 라우터가 소스별 기준으로 감시하기 때문에, 단순한 DoS 공격은 그 소스로부터 발생하는 합법적인 트래픽을 막기 위하여 위장된 소스로 에지 라우터를 범람시키는 것이다.

두 번째로 DoS 공격은 또한 에지 라우터에서 발생할 수 있는데, 이 경우의 에지 라우터는 다른 도메인에 대한 ISP 네트워크의 에지에서의 에지 라우터를 의미한다. ISP가 네트워크 에지에서 다른 도메인들과 SLA를 유지할 수 있기 때문에, 출력 트래픽에 대하여 ISP 네트워크 내부에서 혹은 입력 트래픽에 대하여 ISP 네트워크의 외부에서, SLA를 위반하기 위하여 에지 라우터를 과부하시킴으로써 DoS 공격을 수행할 수 있다. 이 공격은 네트워크 인프라에 대한 지식을 요구한다.

DoS에 대한 세 번째 공격점은 코어 라우터 내부에서 발생하며 네트워크를 위한 SLA에 기초한다. 네트워크 상의 클래스를 과부하시켜 그 클래스로 하여금 더욱 나쁜 성능을 경험하게 할 수 있고 다른 클래스의 트래픽에게도 나쁜 영향을 미칠 수 있다.

3.3.3 제안된 솔루션

이러한 잠재적인 보안 관심사의 결과로, IETF 워킹 그룹은 여러 가지 방법을 제안하였다. 본고에서는 감사(auditing)와 IPSec에 대하여 간략히 기술한다.

1) Auditing : DiffServ 도메인에서 의심스러운 이벤트를 감시하기 위한 방법으로 포함되었다. 감사는 네트워크의 보안과 견고성을 증가시키기 위하여 사용될 수 있다.

2) IPSec : IPSec 터널 모드는 DiffServ 도메인에 대하여 직접 사용할 수 있는 보안을 제공한다. IPSec 터널 모드를 사용하기 위한 몇 가지의 고려할 점은 아래와 같다:

- 코어 라우터는 단지 외부 IP 헤더만 조사한다. 내부 IP 헤더는 도메인의 입구(ingress)

혹은 출구(egress) 노드에서만 조사될 수 있다.

- DiffServ 도메인 사이의 출구 노드는 트래픽 조절(conditioning)을 적용하기 위하여 내부 DS 필드를 수정하는 것이 허용되지 않는다. 만약 수정이 허용된다면, 보안 비용으로 네트워크 적응성을 증가시키는 것이 된다. 따라서 두 개의 DiffServ 도메인 사이의 출구 노드는 입구 노드에서 발견된 적절한 보안을 포함해야 하며, DiffServ 도메인 사이의 노드들의 복잡성을 크게 증가시킨다.

3.4 MPLS 보안[6]

3.4.1 개 요

MPLS(Multi-Protocol Label Switching) 기술은 대규모망에서 고속의 데이터 전송과 QoS 등의 기능을 제공하기 위하여 기존의 라우팅 방식을 기반으로 ATM의 고속 서비스 교환 기능을 결합하여 IP 패킷을 전달하는 방식이다. 이를 위하여 ATM이나 Frame Relay와 같은 계층 2의 교환 기술을 사용하고, 망의 확장성을 제공하기 위하여 계층 3의 라우팅 기능을 접목하였다. MPLS에서는 짧고 고정된 길이의 레이블을 기반으로 패킷을 전송하는데 IP 헤더 처리과정이 모든 홉에서 수행될 필요 없이, 망의 진입점에서만 수행되므로 고속 처리가 가능하다. 그리고 트래픽 공학(Traffic Engineering), VPN 지원 등을 용이하게 할 수 있다.

본 절에서는 MPLS 코어 네트워크는 안전한 방법으로 제공된다고 가정한다. 따라서 비인가된 접속, 코어의 잘못된 구성, 내부 공격 등에 대한 네트워크 요소를 안전하게 하는 기본적인 보안 관심사에 대하여는 기술하지 않는다[6]. 만일 네트워크가 안전하지 않은 경우, MPLS 하부구조 상에 IPSec을 수행할 필요가 있다.

3.4.2 요구사항

이 절에서는 MPLS VPN 구조에서 대표적인 보안 요구사항을 기술한다. 그러나 대부분의 경우 일반적인 MPLS에도 적용된다.

1) 주소 공간 및 라우팅 분리

- 어떤 VPN이라도 다른 VPN과 같은 동일한 주소 공간을 사용할 수 있어야 한다.
- 어떤 VPN이라도 MPLS 코어와 같은 동일한 주소 공간을 사용할 수 있어야 한다.
- 어떤 두 VPN 사이의 라우팅은 독립적이어야 한다.
- 어떤 VPN과 코어 사이의 라우팅은 독립적이어야 한다.

보안 관점에서, 기본적인 요구사항은 어떤 주어진 VPN에서 어떤 호스트로 향하는 패킷이 다른 VPN이나 코어의 같은 주소를 가진 호스트에 도달하는 상황을 피하는 것이다.

2) MPLS 코어 구조의 숨김

MPLS 코어 네트워크의 내부 구조는 외부 네트워크에게 보여서는 안 된다. 예를 들어, 공격자가 만일 코어의 주소를 아는 경우 코어 라우터에 대한 DoS 공격이 훨씬 쉽다. 그러므로 MPLS 코어가 대응되는 계층 2 하부구조처럼 외부 네트워크에게 보이게 하면 안 된다.

3) 공격에 대한 저항

자원에 대한 비인가된 접근을 주는 침입 공격에 대하여는, 네트워크를 보호하는 기본적인 방법이 두 가지 있다. 첫 번째는 남용될 수 있는 프로토콜을 강화하는 것이고, 두 번째는 네트워크를 가능한 한 접근 가능하게 만들지 않는 것이다. 후자는 패킷 필터링이나 방화벽의 사용과 주소 숨김의 결합에 의하여 이루어진다.

DoS 공격에 대한 한 가지 방법은 또한 패킷

필터링이나 주소 숨김에 의하여 타겟 머신에 도착할 수 없도록 하는 것이다.

4) Label spoofing의 불가능성

MPLS는 IP 주소 대신에 라벨(label)을 가지고 내부적으로 동작하기 때문에, 이 라벨이 IP 주소처럼 쉽게 속일 수 있는가에 의문이 발생한다. 외부에서 MPLS 네트워크 내부로 PE(Perimeter Edge)를 통하여 외부에서 틀린 라벨을 가진 패킷을 전송하는 것이 불가능해야 한다.

3.4.3 분석

본 절에서는 3.4.2절에서 나열된 보안 요구사항 관점에서 MPLS 구조를 분석한다. MPLS는 전통적인 계층 2 VPN 서비스에서처럼 완전한 주소와 라우팅 분리를 제공한다. 코어와 다른 VPN의 주소 구조를 숨기며, 현재로선 MPLS 메커니즘을 남용하여 외부에서 코어로 혹은 다른 VPN으로 침입하는 것이 가능하지 않다. 그러나 기존의 프레임 릴레이나 ATM-기반 VPN과는 아주 다르게, MPLS에서는 계층 3에 코어 제어 구조가 있다. 이러한 사실이 산업계에서는 MPLS에 대한 상당한 회의론을 야기 시켰다. 왜냐하면, 이 설정이 구조를 다른 VPN이나 인터넷으로부터의 DoS 공격에 대하여 개방할 수 있기 때문이다.

[6]에서는 상응하는 ATM이나 프레임 릴레이 서비스와 같은 보안 수준으로 MPLS 하부구조를 안전하게 할 수 있다는 것을 보여준다. MPLS VPN 구조에서, 다른 VPN을 직접 침입하는 것이 가능하지 않고, 단지 가능한 방법은 MPLS 코어를 공격하여 그곳에서 다른 VPN 공격을 시도하는 것이다. MPLS 코어는 두 가지의 기본적인 방법으로 공격될 수 있다:

- PE 라우터 직접 공격
- MPLS 신호 메커니즘 공격

MPLS 코어의 주소 구조를 숨기는 것이 가능하기 때문에, 공격자는 자신이 공격하고자 하는 코어 내의 어떤 라우터의 IP 주소를 모른다. 공격자는 이제 주소를 추측하여 이 주소로 패킷을 전송한다. 그러나 MPLS의 주소 분리로, 각 입력 패킷은 고객의 주소 공간에 속하는 것으로 취급된다. 그리하여 IP 주소 추측을 통하여도 내부 라우터에 도달하는 것이 불가능하다. 이 규칙은 PE 라우터의 피어 인터페이스인 경우에 대하여 단지 예외가 있다.

공격에 대한 저항 능력을 요약하면 다음과 같다. 하나의 VPN으로부터 다른 VPN이나 코어를 침입하는 것은 가능하지 않다. 그러나 PE 라우터에 대하여 DoS 공격을 실행하기 위하여 라우팅 프로토콜을 이용하는 것은 이론적으로 가능하다. 이것이 다른 VPN에 대신 부정적인 영향을 끼칠 수 있다. 그리하여 PE 라우터는 극도의 보안이 요구되며, 특히 CE 라우터에 대한 인터페이스 상에서 그렇다. 라우팅 프로토콜의 포트에 대하여만 그리고 CE 라우터로부터 만 접근을 제한하기 위하여 ACL(Access Control List)이 구성되어야 한다. 라우팅 프로토콜에서의 MD5 인증이 모든 PE/CE 피어링에서 사용되어야 한다. 이러한 잠재적인 DoS 공격의 소스를 추적하는 것이 쉽게 가능하다.

3.4.4 보완점

[6]에서는 MPLS가 제공하지 못하는 것으로 다음과 같이 기술하고 있다:

- 코어의 잘못된 구성과 코어 내부 공격에 대한 보호

잘못된 구성의 위험을 피하기 위하여, 장비는 구성하기 쉬어야 한다. 내부 공격의 위험을 피하기 위하여 MPLS 코어 네트워크가 적절히 보호되어야 한다. 이 보안은 네트워크 요소 보안, 관리 보안, 서비스 제공자 인프라의 물리적 보안,

서비스 제공자의 설치에 대한 접근 제어와 다른 표준 서비스 제공자 보안 메커니즘들이 있다.

• 데이터 암호화, 무결성, 기원 인증

MPLS 자체로는 암호화, 무결성, 인증 서비스를 제공하지 않는다. 이러한 특징이 필요하면, IPSec이 MPLS 인프라 상에 사용되어야 한다.

• 고객 네트워크 보안

고객 네트워크의 전반적인 보안을 위하여 코어 네트워크의 보안뿐만 아니라 연결의 내외부 및 모든 입구점에서의 보안이 요구된다.

4. 표준화 동향

본 절에서는 ITU-T X.805의 보안 개념에 대하여 소개하고자 한다[14]. ITU-T X.805에 의하여 표준화된 보안 구조는 서비스 제공자, 엔터프라이즈 및 소비자의 전역적인 보안 문제를 다루기 위하여 만들어졌으며, 무선, 광 및 유선 음성, 데이터 및 통합 네트워크에 적용될 수 있다. 이

〈표 1〉 보안 위협에 대한 보안 디멘전의 매핑

보안 디멘전	보안 위협				
	정보나 다른 자원의 파괴	정보의 오손, 변조	정보 및 다른 자원의 절도, 제거, 손실	정보 노출	서비스 차단
접근 제어	Y	Y	Y	Y	
인증			Y	Y	
부인방지	Y	Y	Y	Y	Y
데이터 기밀성			Y	Y	
통신 보안			Y	Y	
데이터 무결성	Y	Y			
가용성	Y				Y
비밀성				Y	

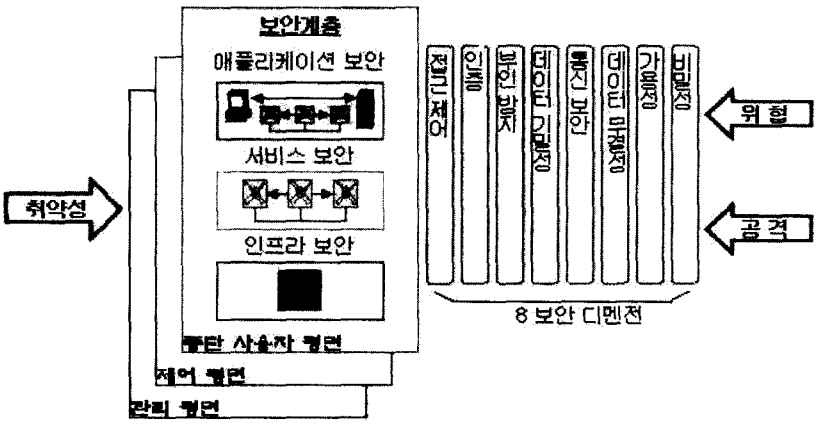

그림 1. 종단간 네트워크 보안을 위한 보안 구조[14]

보안 구조는 네트워크 인프라, 서비스 및 애플리케이션의 관리, 제어와 사용에 대한 보안 관심사를 기술한다. 보안 구조는 네트워크 보안의 포괄적인, 탑-다운, 종단간 관점을 제공하며 보안 취약성을 탐지, 예측, 교정하기 위하여 네트워크 요소, 서비스와 애플리케이션에 적용될 수 있다. 분명히, X.805의 보안 구조는 부가적인 보안 개발을 요구하는 통합망 관점에 적용될 수 있다.

표 1은 보안 위협에 대한 보안 디멘전(security dimension)의 매핑(mapping)을 제공한다. 매핑은 각 보안 관점에 대해서 동일하다. 블록 안에 있는 Y자는 특정한 보안 위협이 해당 보안 디멘전에 의하여 대항한다는 것을 나타낸다.

그림 1은 종단간 네트워크 보안을 위한 보안 구조를 보여준다.

보안 평면(security plane)은 보안 디멘전(security dimension)에 의하여 보호되는 네트워크 활동의 어떤 형태이다. 이 권고안은 세 가지 형태의 보호 활동을 나타내기 위하여 세 개의 보안 평면을 정의한다. 보안 평면은 관리 평면, 제어 평면, 종단 사용자 평면으로 구성된다. 이 보안 평면이 각각 네트워크 관리 활동, 네트워크 제어나 신호 활동, 그리고 종단 사용자 활동과 관련 있는 특정한 보안 필요성을 기술하고 있다. 보안 요소와 함께 보안 구조를 보여주며 위에서 기술된 보안 위협을 나타낸다. 그림 1은 포괄적인 보안 솔루션을 제공하기 위하여 각 보안 계층의 각 보안 평면에서의 보안 디멘전에 의한 네트워크 보호 개념을 나타낸다. 주어진 네트워크의 보안 요구사항에 따라서 모든 구조 요소가 구현될 필요가 없을 수 있다.

그림 2는 보안 프로그램에 대한 보안 구조의 적용을 보여준다.

보안 구조는 그림 2에서처럼 보안 프로그램의 모든 측면과 과정에 적용될 수 있다. 보안 프로그램은 기술 이외에 정책과 절차로 구성되며, 수명의 과정에 걸쳐 세 단계를 통하여 진행된다. 세 단계는 정의 및 계획 단계, 구현 단계와 유지보수 단계로 이루어진다. 그림 3은 표 형태의 보안 구조를 제시하며 네트워크를 안전하게 하기 위한 방법론적 접근을 보여준다. 그림에서 보여주듯이, 보안 평면과 보안 계층의 교차는 8개의 보안 디멘전을 고려하기 위한 유일한 관점을 나타낸다. 9개의 각 모듈들이 특정 보안 평면에서 특정 보안 계층에 적용되는 8개의 보안 디멘전을 결합한다.

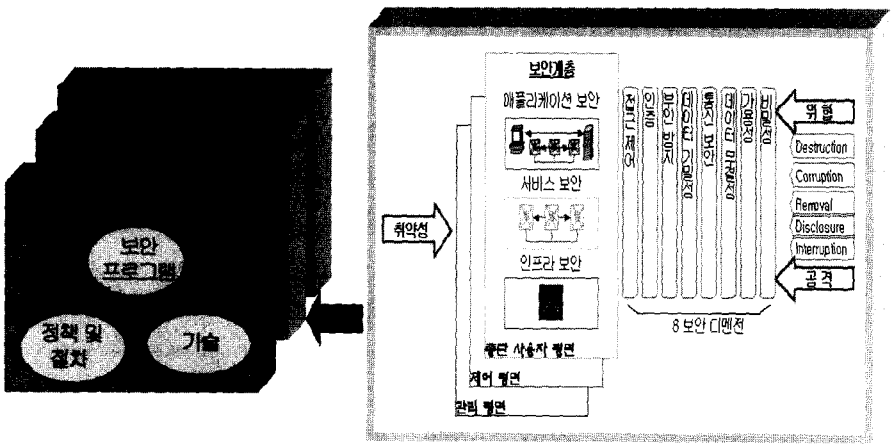

그림 2. 보안 프로그램에 대한 보안 구조의 적용[14].

5. 국내 추진 계획

본 절에서는 국내의 BcN 구축 기본 계획에 의한 통합망 보안 기능 고도화에 대하여 간략히 기술하고자 한다[1]. 우리나라에서도 정보보호 기술의 고도화 및 정보보호 체계 통합화를 통하여 안전하고 신뢰성 있는 건전한 사이버 네트워크 환경 구축을 추진하고 있다. 국내에서 계획하고 있는 통합망 보안기능 고도화를 위한 망 구축 방안은 아래와 같다[1]:

- 망의 신뢰성과 안정성 확보를 위한 out-of-band 신호채널과 생존성 보장을 위한 침입감내(Intrusion Tolerant) 네트워크 구축
- 개별망 단위의 정보보호 시스템을 상호 연

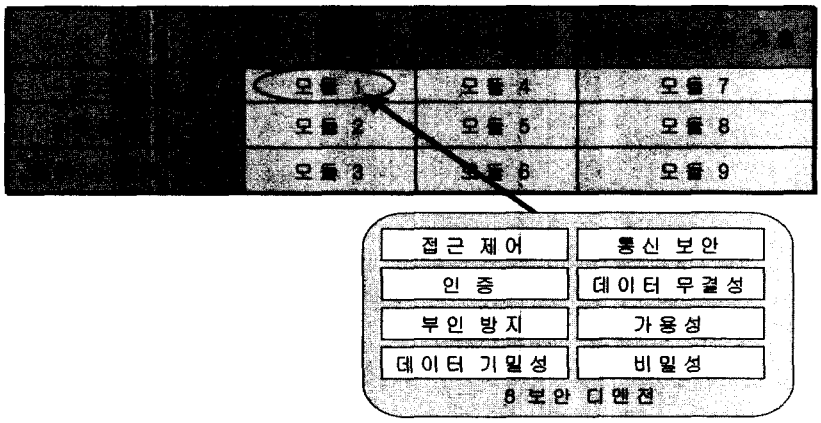

그림 3. 표 형태의 보안 구조[14]

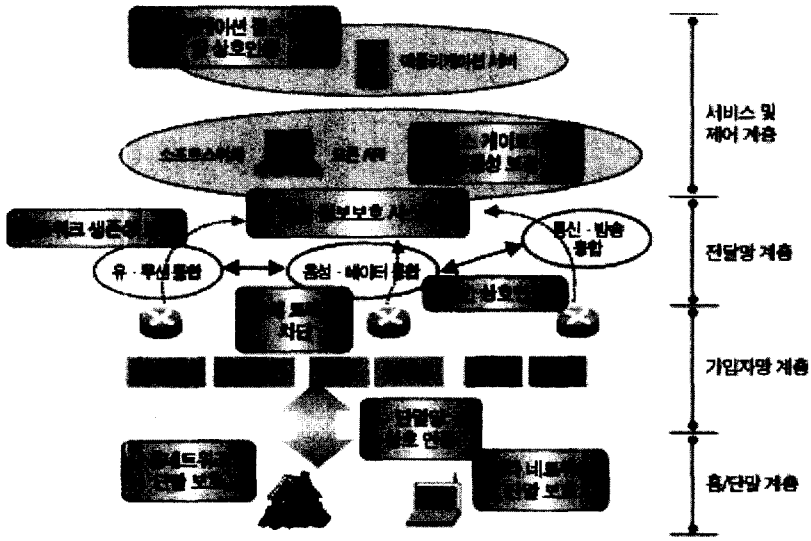

그림 4. BcN 보안망 체계도[1]

동할 수 있는 통합 정보보호 시스템을 단계적으로 발전: 통신망간 및 통신망과 단말간 상호인증, 불건전 정보 사전 차단, 이상 트래픽 감시·대응을 통한 네트워크 안정성 및 생존성 보장

- 정보보호 단위 기능간의 종합적이고 유기적인 연동을 통해 침해 탐지·차단·대응·복구기능을 자동 수행하는 보안 환경 구축

그림 4는 BcN 보안망 체계도를 보여준다.

표 2는 단계별 보안기능 고도화 방안을 보여준다.

표 2에서 의하면, 1단계에서는 DDoS 및 웜 해킹 대응, 과다 트래픽 감시, 홈네트워크 단말 보호 등의 기술이 개발될 예정이며, 수 Giga 급 보안장비가 BcN 전달망에 적용될 전망이다. 2단계에서는 네트워크 통합형 해킹 대응 체계가 구축될 예정이며, 또한 유해 트래픽 차단 기술과 수십 기가급 고성능 보안 장비가 도입될 것으로 보이며, 생체 인증이 고도화되고 네트워크 통합형 보안 관리 시스템이 처음으로 도입되는 등 보안 기능이 점차 고도화될 전망이다. 3단계에서는 통신·방송 융합형 해킹 대응 및 통합 보안 관리 시스템이 개발되어 적용될 예정이며, 비정상 트래픽 제어 기술이 개발되고 수백 기가급 고성능·고기능 보안장비 등이 적용되어 고도화된 보안 관리 시스템이 완성될 예정이다.

이의 효과적인 추진을 위한, 주요 추진 과제를 요약하여 기술하면 다음과 같다[1]:

- 기술 개발 및 표준화
  - 고성능 통합 네트워크 정보보호 기술 개발
  - 주요 장비 보호 기술 개발
  - 통합 인증 기술 개발
  - 정보보호 기술 표준화
- 통합보안관리 체계 구축
  - 유선·무선·방송 통합망 트래픽 종합 모니터링 체계 구축
  - 사이버 공격 자동 침입탐지·분석·대응 보안관리 시스템 구축
  - 민·관 공조체계를 강화한 침해사고 긴급대응 체계 구성·운영

〈표 2〉 단계별 보안기능 고도화 방안[1]

구분	상호인증 및 접근제어	네트워크 생존성 보장	BcN 시스템 보호
1단계 (2004~05)	- 단말·망 상호인증 - PKI 고도화	- DDoS/Worm 해킹 대응 - 과다 트래픽 감시 - 수 Giga급 보안장비 - 감시기반 보안관리 시스템	- 홈네트워크 단말 보호 - DNS 보안 - DB 보안
2단계 (2006~07)	- 망간 상호 인증 - 생체인증 고도화	- 네트워크 통합형 해킹 대응 - 유해 트래픽 차단 - 수십 Giga급 고성능 보안장비 - 네트워크 통합형 보안 관리 시스템	- 유·무선 통합형 단말 보호 - 서비스 게이트웨이보안
3단계 (2008~10)	- 통신·방송 상호 인증 - 통합인증 서비스 보장	- 통신·방송 융합형 해킹 대응 - 비정상 트래픽 제어 - 수백 Giga급 고성능·고기능 보안장비 -통신·방송 융합형 통합 보안 관리 시스템	- 통신·방송 융합형 단말 보호 - BcN 노드 보안

• 정보보호 법 · 제도 개선

6. 맺음말

BcN 전달망의 특징은 QoS 보장, 보안 기능 제공, IPv6 수용, 개방형 망 구조로 요약할 수 있다. BcN을 위한 QoS를 제공하기 위한 구조로 통합 서비스 모델인 RSVP, DiffServ 모델, 그리고 MPLS가 있다. 보안은 현대의 정보 시스템에서 아주 중요한 부분이다. BcN에서 QoS를 안전하게 제공하기 위하여 BcN QoS 구조에서 보안 메커니즘에 대한 연구가 필요하다. 이에 따라 본 고에서는 BcN에서 안전한 QoS 제공을 위한 SQoS 메커니즘에 대하여 기술하였다.

먼저 BcN 보안 특징에 대하여 살펴보고, QoS 구조에서 보안 메커니즘을 도입하기 위한 방안으로, RSVP 프로토콜의 취약점을 살펴보고 대응방법에 대하여 기술하였다. 그 다음에 DiffServ의 정확한 운영에 중요한 보안 관심사를 나타내는 여러 가지의 핵심 신뢰 영역에 대하여 제시하였다. 본 고에서는 또한 MPLS 보안의 여러 가지 측면에 대하여 토의하였다. 표준화 동향에서는 통합망 관점의 보안 구조 개발에 적용될 수 있는 ITU-T X.805에 대하여 살펴보았다. 마지막으로 국내 추진 계획에서는 정보통신부의 광대역 통합망 구축 기본 계획에서 통합망 보안 기능 고도화에 대한 내용을 소개하였다. 정보통신 인프라 보호에 대한 보다 자세한 내용은 한국통신학회지 9월호에서 소개하고자 한다.

참 고 문 헌

[1] 정보통신부 BcN 구축 기본 계획(2. 통합망 보안기능 고도화), pp76-83, 2004년 2월, 한국전산원.

[2] Allan J. Albrecht, Measuring application development, In Proc. of IBM Applications Development Joint SHARE/GUIDE Symposium, pp83-92, Monterey, CA, USA, 1979.

[3] M. Behringer, Analysis of the Security of BGP/MPLS IP VPNs, Internet Draft, Jan. 2004.

[4] Jonna Bengtsson, Magnus Falk, "Distributed Denial of Service", TDDC03 - Information Security, May 6, 2003, Linkoeping University.

[5] Richard Carlson, T. H. Dunigan, Russ Hobby, Harvey B. Newman, John P. Streck, Mladen A. Vouk, "Strategies & Issues: Measuring End-to-End Internet Performance", http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703532

[6] Cisco Systems, White Papers, Security of the MPLS Architecture, Cisco Systems Inc.

[7] B. Gamm, B. Howard, O. Paridaens, "Security features required in an NGN", Alcatel Telecommunications Review, 2nd Quarter 2001, pp.129-133.

[8] Evdoxia Spyropoulou, Timothy E. Levin, and Cynthia E. Irvine, Calculating costs for quality of security service, In Proc. of the 16th Annual Computer Security

Applications Conference, pp334-343, New Orleans, Louisiana, USA, Dec. 11-15, 2000.
[9] Ravi Sinha, MPLS-VPN Services and Security, GSEC Practical Ver 1.4b, Option 1, SANS Institute 2003.
[10] A. Striegel, "Security Issues in a Differentiated Services Internet".
[11] "Telecommunications and Internet Protocol Harmonization over Networks(TIPHON) Security; Threat Analysis", DTR/TIPHON - 08002 V0.1.9 (2001-02-09).
[12] Stefan Lindskog, Erland Jonsson, "Introducing Security in QoS Architectures".
[13] Tsung-Li Wu, S. Felix Wu, Zhi Fu, He Huang, Feng-Min Gong, "Securing QoS: Threats to RSVP Messages and their Countermeasures".
[14] ITU-T X.805 Rec., Security architecture for systems providing end-to-end communications.

전 용 희

1971. 3~1978.2 고려대학교 전기공학과
1985. 8~1987.8 미국 플로리다 공대 대학원 컴퓨터공학과
1987.8~1992.12 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978. 1~1978.11 삼성중공업(주)
1978.11~1985.7 한국전력기술(주)
1989.1~1989.6 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989.7~1992.9 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA
1992.10~1994.2 한국전자통신연구원 광대역통신망연구부 선임연구원
1994.3~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2000.1~현재 한국통신학회 학회지 편집위원
2001.3~2003.2 대구가톨릭대학교 공과대학장 역임
2004.2~현재 한국전자통신연구원 정보보호연구단 초빙연구원

<관심분야> 네트워크 보안, 통신망 자원관리 및 성능분석, QoS 보장 기술