情 報 保 護 學 會 誌
第 15 卷 第 3 號, 2005. 6

BcN 인프라 정보보호

전 용 희*, 장 종 수**

요 약

광대역 통합망(BcN: Broadband convergence Network)에서 대역폭의 증가와 서비스의 통합으로 보안의 중요성이 빠르게 증가하고 있다. 그러므로 보안은 BcN에서 다루어져야 할 중요한 문제의 하나로 인식되어야 한다. BcN과 같은 QoS-aware 통신시스템에서 사용자는 원하는 서비스 품질 수준의 보장을 위하여 여러 가지의 서비스 클래스 중에서 선택할 수 있다. 그러나 보안은 아직 이런 QoS 구조에서 하나의 파라미터로 인정되지 않고 있으며, 보안-관련 서비스 클래스도 정의된 바 없다. 본고에서는 BcN 구조에서 발생할 수 있는 보안 취약성을 분석하고 BcN 인프라 정보보호를 위하여 관련 기술, 표준화, 국내 동향 등에 대하여 기술하고자 한다.

Ⅰ. 서 론

인터넷에서 제공되는 전통적인 "최선(best-effort)" 서비스는 네트워크 트래픽의 상세하고 일관성 있는 수준의 QoS를 지원하기 위하여 설계되지 않았다. 광대역 통합망(BcN: Broadband convergence Network)이란 통신·방송·인터넷이 융합된 품질보장형 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.

정보통신부가 추진하고 있는 IT839 프로젝트에서 3대 인프라로 BcN, IPv6, USN(Ubiquitous Sensor Network)가 있다. BcN과 같은 광대역 통합망 환경에서는 보안침해 사고가 발생하면 그 피해가 전체 네트워크로 광범위하게 확산되어 심각한 통신피해가 우려되고, 사이버 공격의 추세가 지능화, 악성화 되고, 다양한 경로를 통하여 통신망에 쉽게 접근이 가능하여 지기 때문에 네트워크 보안을 위한 대책이 절실히 필요하다. 2003년 1.25 인터넷 침해사고 이후 국내에서는 정보보호 대책을 본격적으로 강구하여 추진중이다.

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] BcN 보안 대책을 위한 정보보호 기술의 고도화 및 정보보호 체계의 통합화를 통하여 안전하고 신뢰성 있는 건전한 사이버 네트워크 환경 구축을 추진하고 있다.

본고에서는 BcN 인프라에서의 보안 취약성, BcN 구현을 위하여 고려되어야 할 보안 고려사항들을 살펴보고, BcN 인프라 보호를 위한 기술과 특징, ITU-T X.805 권고안에서 기술하고 있는 종단간 보안을 위한 구조와 X.805의 보안 개념을 BcN에 적용할 수 있는 방안, secure QoS 개념, 마지막으로 BcN 구축 기본 계획에서 보안 기능 고도화 방안에 대하여 소개하고자 한다.

Ⅱ. BcN 보안 취약성과 대응책

BcN과 같은 QoS-aware 통신시스템에서, 사용자는 각각 다른 신뢰성, 예측성과 효율성 정도를 가지고

* 대구가톨릭대학교 공과대학 컴퓨터정보통신공학부 (yhjeon@cu.ac.kr)
** 한국전자통신연구원 정보보호연구단 네트워크보안그룹 (jsjang@etri.re.kr)

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 의미 한다. 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)로 구성되어 있다는 점이다. 그러나 이 세 개의 속성들은 하부시스템이나 통신 채널들의 다르고, 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 한 명은 높은 수준의 무결성을 요구할 수 있다.

2.1 보안 취약성과 요구사항

BcN과 같은 통합망 환경에서 개별망의 피해가 BcN으로 연결된 모든 네트워크로 확산될 가능성이 더욱 높아진다. 네트워크 혹은 서비스 제공자는 위협 분석과 위험 평가의 결과를 근거로, 어떤 보안 대책을 수립할 것인지를 결정해야 한다. 다른 형태의 전송 구조를 고려하여, BcN에서 발생할 수 있는 주요한 위협의 형태로는 다음과 같은 것이 있다.[2]

- 서비스 거부(Denial of Service: DoS): 다른 사용자에게 네트워크 자원이 이용가능하지 못하도록 데이터로 네트워크를 범람시킨다.
- 도청: 송신자와 수신자 사이의 정보를 가로채어 비밀성을 위협한다.
- 해킹 혹은 침입 공격: 침입자가 어떤 지역이나 자원의 집합에 불법적인 접근을 획득한다.
- 바이러스 및 웜: 네트워크상에 확산되어 정보를 파괴하고 변조하며 전파된다.
- 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.

ITU-T Rec. X.800에서 기술하고 있는 위협은 다음과 같다.

- 정보와 다른 자원의 파괴
- 정보의 오손 혹은 변조
- 정보와 다른 자원의 절도, 제거 혹은 손실
- 정보의 노출
- 서비스의 차단

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[3]의 위협 분석이 지침서로 사용되었다.[2] 일반적인 보안 요구사항은 다음과 같다.

- 계정성(accountability)
- 신원 검정
- 인증

이와 같이 BcN 인프라 정보보호를 위하여, 네트워크의 인입점에서 네트워크 위협을 능동적으로 탐지하고 대응할 수 있는 통합 보안 관리 기술, 네트워크의 발전 속도를 고려한 고성능 네트워크 위협 대응 기술, 알려진(known) 침입 공격에 대한 탐지 기술과 알려지지 않은(unknown) 침입에 의한 과다 트래픽(excessive traffic) 탐지 기술, 유해 트래픽(malicious traffic)에 대한 차단 및 대역폭 제어 기술 등이 요구된다.[4]

2.2 대응책

대응책은 일반적으로 예방적(preventive)과 탐지적(detective)으로 분류할 수 있다. 상기 위협에 대처할 수 있는 일반적인 대응책은 다음과 같다.[2]

- 인증(authentication)
- 디지털 서명
- 접근 제어
- 가상사설망(VPN)

· 암호화
· 침입탐지 및 방지
· 감사(auditing) 및 기록(logging)
· 부인방지 대책

Ⅲ. BcN 인프라 보호 기술

본 장에서는 위에 기술된 대응책들 중에서 침입탐지 및 방지 기술에 대하여 기술한다.

3.1 침입탐지 기술

침입탐지시스템(IDS: Intrusion Detection System)은 권한이 부여되지 않거나 승인되지 않은 네트워크 행위를 식별하고, 평가하고, 보고하는 것을 도와주는 도구, 방법, 자원으로 정의될 수 있다.[5] 침입탐지시스템은 전체적인 보안 시스템 구성의 일부에 지나지 않는다. 방화벽, IDS, IPS(Intrusion Prevention System) 모두가 네트워크로의 침입을 경보하고 방지하기 위하여 함께 사용된다. 다만 이들은 다른 기술을 사용할 뿐이다.

상업용 네트워크 기반 IDS(NIDS: Network-based IDS)는 1990년 중반부터 사용되고 있다.[6] 침입탐지를 위하여 센서를 사용하는데, 초창기에는 센서가 패킷을 조사할 수 있는 속도보다 네트워크 속도가 더 빠를 수 있었기 때문에, 성능이 한 가지 문제였다. 1 세대 상업용 NIDS는 순수한 시그니처-기반(Signature-based) 모델이었다. 센서가 각 네트워크 세그먼트에 위치하여 "알려진" 공격 시그니처의 데이터베이스에 대하여 네트워크 패킷을 모니터하여 조사한다. 새로운 위협이 발생하면, 해당 익스플로잇(exploit)을 탐지하기 위한 시그니처를 생성할 필요가 있다.

순수 시그니처 기반 시스템의 문제점으로 다음과 같은 몇 가지가 있다. 첫째는 패킷 시그니처가 다른 네트워크 트래픽에 유일하지 않기 때문에 유효한 트래픽에 대하여도 경보를 발생할 수 있고, 두 번째는 보안 관리자가 알 필요도 없는 이벤트에 대하여 경보를 발생할 수 있고, 세 번째는 알려지지 않은 공격은 탐지를 할 수 없다는 것이다. 다시 말하면, 이 방법에서는 발견되는 취약성의 증가에 따라서 익스플로잇의 수도 크게 증가하게 된다. 따라서 증가되는 시그니처 데이터베이스로 인하여 센서의 성능 문제가 더욱 심각하게 되는 문제가 발생한다.

이 문제를 해결하기 위하여, 2세대 NIDS는 시그니처 대신에 룰(rule)을 사용한다. 여기서는 익스플로잇 시그니처 대신에 패킷 시그니처를 규칙의 집합에 대하여 비교한다. 패킷 시그니처 탐지에서, 트래픽을 정확하게 처리하기 위하여, 데이터의 오번역을 제거하기 위한 기술이 사용되어야 한다. 이 기술들로 다음과 같은 것이 있다.[7]

· IP-defragmentation-패킷의 프레그먼트들을 패킷으로 적절히 결합하는 능력
· TCP 재결합- 중복된 데이터를 제거하면서, 바른 순서대로 TCP 세그먼트들을 적절히 재결합하는 능력
· 플로(flow) 추적- 플로를 추적하여 하나의 통신 세션으로 관련시키는 능력
· 정규화(normalization)-재결합된 메시지로부터 부호화된 표현과 특수 문자를 번역하고, 필요한 경우 제거하는 능력

대부분의 NIDS는 패킷 시그니처 탐지를 사용하는데, 이것은 공격 패턴과의 매치를 조사하기 위하여 플로(flow) 안의 모든 패킷의 바이트 정보를 보아야 한다는 것을 의미한다. 따라서 다음과 같은 두 가지의 문제가 있다.

· 전체 플로가 조사될 필요가 있기 때문에 성능이 심각하게 저하된다.
· 더 많은 데이터를 시스템이 조사할수록 시그니처가 관련 없는 데이터에 매치될 가능성이 많아진다는 단순한 사실에 기초하면, 오탐이 발생할 가능성이 많아진다.

이러한 규칙-기반 시스템은 공격 외에도 네트워크 정책 위반에 대한 탐지에도 사용될 수 있다.

2세대 NIDS의 성능과 정확성 결핍 문제를 극복하기 위하여, 제 3세대 NIDS는 공격을 탐지하기 위하여 프로토콜 이례(anomaly)를 사용한다. 프로토콜 이례 NIDS는 네트워크상에서 허용되는 프로토콜들의 적절하지 않은 사용을 관찰함으로써 공격을 식별할 수 있다. 프로토콜 이례 탐지(protocol anomaly detection)의 장점은 다음과 같다.[7]

- 공격이 프로토콜 표준으로부터 벗어난다는 사실에 기초하여, 알려지지 않은 새로운 공격을 탐지할 수 있다.

- 다른 탐지 방법을 구현한 시스템을 우회하는 공격을 탐지한다.
- 시그니처-기반 시스템을 회피하기 위하여, 공격의 강도에 영향을 주지 않고, 알려진 공격 패턴의 형식을 변경한 약간 수정된 공격을 탐지한다.

이에 대한 예로써 FTP bounce 공격 탐지와 서류화 되지 않은 버퍼 오버플로 공격 탐지가 있다. 이 방법은 버퍼 오버플로 공격 같은 의심스러운 행위를 탐지하는데 매우 효율적이다. 이 시스템의 문제는 모든 응용 개발자가 철저하게 표준을 준수하지 않기 때문에, 부적절하게 통신하는 정당한 트래픽에 대하여 경고를 발생하는 것이다.

프로토콜 이례 탐지의 일부로서 수행되는, stateful inspection과 프로토콜 분석을 이용하여 공격 패턴을 식별하는 stateful 시그니처 탐지 방법이 있다. 스테이트풀 시그니처는 전송 시에 각 데이터 바이트의 문맥과 클라이언트와 서버의 상태를 이해한다. 이것은 각 시그니처가 관련 있는 통신 상태에 따라서, 단지 관련된 데이터 바이트와 비교될 수 있다는 것을 의미한다. 다시 말하면, 스테이트풀 시그니처는 공격이 손상을 일으킬 수 있는 통신 상태에서의 공격만 조사함으로써, 성능을 상당히 개선시키고 오탐을 감소시킨다.

최근 NIDS는 공격을 결정하기 위하여 순수한 통계적 분석을 사용한다. 시스템은 통상적인 통신 패턴을 학습하고 비정상에 대하여 경보를 발생할 수 있다. 다른 NIDS의 형태에 비하여 이런 형태의 시스템은 자산에 대한 비전통적인 공격을 탐지할 수 있는 능력에 있다. 그러므로 내부자 공격의 감시에도 사용 가능하다.

현재 가장 널리 사용되는 NIDS 범주는 하이브리드 접근이다. 이 방법에서는 시그니처 기반, 규칙 기반, 프로토콜 어노멀리 탐지와 같은 여러 가지 방법의 탐지에 기초하여 경보를 생성함으로써, 오탐율을 줄이는데 도움을 줄 수 있다.

호스트 기반 침입탐지시스템(HIDS: Host-based IDS)은 호스트 상에서 발생하는 어떤 이벤트에 의존한다. 초창기 HIDS는 공격을 결정하기 위하여 "파일 감시"의 개념을 사용하였다.[6] 이것은 중요한 서버 상에서 중요한 시스템 파일의 변경을 감시하기 위한 것이다. 파일 변경이 발생하면, 경보를 발생하고 시스템 관리자에게 통보한다. 다음 세대의 HIDS는 보안 관리자로 하여금 시스템과 자원 사용에 대하여 엄격한 정책을 설정하도록 허용하였다. HIDS 에이전트는 권한이 없는 사용자로부터 운영체제에서 시스템 registry와 이벤트 로그들의 변경에 대하여 감시하도록 맞출 수 있다. 모든 호스트 행동들이 사용을 위한 룰 셋(rule set)에 대하여 비교된다. 정책이 지켜지지 않으면, 경보를 발생하거나 자동 대응을 할 수 있게 된다. 이 방법은 중요 호스트 상에서 도메인 같은 보안 정책을 실행하기 위하여 효과적이다. 단점은 정책의 구성이다. 경보를 개시하기 위하여, 시스템 관리자는 HIDS 관리 안의 모든 요구되는 행위를 구성해야 한다. HIDS의 근본적인 문제는 항상 침입 발생 후 사후 조치를 취한다는 것이다.

3.2 침입방지 기술

침입방지시스템(IPS)도 IDS와 마찬가지로 호스트 기반과 네트워크 기반 시스템으로 분류된다.[8,9] 호스트 기반 IPS(HIPS: Host-based IPS)는 가트너의 정의에 의하면, 우선 소프트웨어 제품이어야 하고, 방화벽 규칙 집합과 같은 정책이나 정상/비정상 접근에 대한 학습을 통해 취약한 응용 프로그램을 보호할 수 있어야 하며, 커널과 독립적으로 작동하는 방식과 함께 동작하는 방식으로 구분된다. 전자는 시그니처와 행위 기반 분석 알고리즘을 이용 특정 규칙에 위배되는 이벤트를 필터링하는 제품들로 분류할 수 있다. 후자는 대부분 접근제어 기능을 가진 트러스트(trust) 운영체제 제품들로 분류할 수 있다.

역시 가트너의 정의에 의하면, 네트워크 기반 IPS (NIPS)는 침입방지 능력과 빠른 대응 속도를 위하여 네트워크 라인상에 위치한 제품이어야 하며, 세션 인식 감시(session aware inspection)를 지원할 수 있는 시스템이다. 그리고 다양한 종류의 방지 방법 및 방식(시그니처, 프로토콜의 비정상 행위 탐지)을 통하여 악의적인 세션을 차단하는 것도 필수적이다.

[10]에서는 침입방지시스템의 형태를 다음과 같은 다섯 가지의 범주로 구분하여 기술하고 있다.

- 인라인 네트워크 침입탐지시스템
- L7 스위치
- 애플리케이션 방화벽/IDS
- 하이브리드 스위치:
- 거짓 애플리케이션

3.2.1 네트워크 기반 침입방지시스템

NIDS는 네트워크 트래픽을 엄격히 감시하기 위하여 설계된 하나의 솔루션이며, 트래픽을 통과시킬지

아닐지에 대하여 아무런 결정을 내리지 않는다. 반면에 NIPS는 공격 탐지에 기초하여 트래픽을 통과시킬지 아닐지에 대하여 결정을 내릴 수 있는 인라인 장치이다. 원하지 않는 트래픽을 차단할 수 있는 능력이 주요한 차이점이다.

원하지 않는 공격 트래픽을 막기 위하여, 초창기에는 방화벽과 NIDS 시스템을 결합하여 사용하였다. 탐지된 공격에 기초하여, NIDS 시스템은 경계 게이트웨이에서 공격자를 차단하기 위하여 on the fly로 새로운 방화벽 접근 통제 규칙을 추가할 수 있었다. 이것은 여러 가지 이유로 성공적이지 못하였다. 이 방법이 시도된 때에, NIDS는 높은 오탐율을 가지고 매우 부정확하였다. 이와 같은 방법으로 방화벽을 통제하는 것은 보안을 거의 증가시키지도 못하였으며, 높은 확률로 정당한 네트워크 트래픽을 차단하였다. 이런 형태의 시스템들은 전체 IP 주소에 의하여 서비스를 받을 수 있든지 아니면 차단하기 위하여 방화벽에 접근통제 규칙을 추가하기 때문에, NAT(Network Address Translation)를 사용하여 하나의 public IP를 사용하는 경우 모든 사용자들이 차단되는 문제가 발생하게 된다.

현재의 NIPS는 원하지 않는 트래픽을 막기 위하여 전혀 다른 접근을 가진다. 초창기 시스템에서 사용된 접근 통제 방지 대신에 패킷 레벨 탐지 및 방지를 사용함으로써 공격 세션으로부터 원하지 않는 패킷들만 탈락시킬 수 있다. 이것이 NIPS 시스템이 성공적인 하나의 주요한 이유이다.

어떻게 NIPS가 공격을 탐지하는가는 여전히 중요하며, 아직도 오탐 문제가 여전히 현실로 남아있다. 현재의 NIPS는 공격 트래픽을 탐지하기 위하여 하이브리드 접근 방법을 사용한다. 그러나 주요한 차이는 익스플로잇이 아닌 취약성에 기초한 시그니처를 사용하는 것이다. 발견되는 모든 취약성에 대하여 많은 수의 익스플로잇이 방출될 수 있는데, 취약성에 대한 시그니처를 작성함으로써 NIPS는 실제 익스플로잇이 나오기 전에 보호를 추가할 수 있게 된다. 또한 이렇게 함으로써 검색 엔진에서 요구되는 데이터양이 상당히 감소되도록 도와준다.

전통적인 보안 모니터링과 대응 역할에서, NIDS는 공격에 대하여 보안 관리자에게 경보를 보내고, 관리자는 수동적으로 공격에 대응하게 된다. 그러나 NIPS에서는 자동 대응이 가능하고, 필요한 경우 보고서를 통하여 자동 대응을 검정할 수 있기 때문에 관리자 업무가 감소되는 장점도 있다.

3.2.2 호스트 기반 침입방지시스템

호스트 기반 침입방지시스템(HIPS)은 시장에서 가장 새로운 제품이다. HIPS 에이전트는 보호되는 호스트의 운영체제 위에서 수행되기 때문에 "최종 계층(last layer)" 보안 모델이라고 말할 수 있다. HIPS는 호스트 상의 공격을 탐지하고 그것이 실행되기 전에 공격 프로세스를 막을 수 있다.

공격 탐지 방법도 전통적인 HIDS 모델로부터 변화하였다. HIPS는 조치를 취하기 전에 더 이상 서비스가 이벤트 로그를 생성하거나 시스템 파일이 변경되는 것을 요구하지 않는다. 실제적인 탐지 방법은 제조사에 따라 다르지만, 공격을 탐지하기 위한 통상적인 방법은 규칙-기반 접근이다. HIPS 도구는 제품과 함께 전달되는 "허용/비허용 행위" 규칙의 미리 정해진 목록을 가지고 있다. 이런 규칙들은 어떻게 운영 체제나 애플리케이션이 행동해야 하는지를 알고 있다. 만약 애플리케이션이 "오동작"을 시작하면 규칙이 트리거되고 공격 프로세스는 해를 끼치기 전에 커널 레벨에서 kill된다.

규칙-기반 HIPS를 받치는 이론은, 취약성과 익스플로잇은 높은 속도로 항상 변하지만, 그러한 익스플로잇이 수행하는 행동은 상당히 일정하다는 사실이다. 예를 들어, 인터넷의 첫 번째 웜인 1988년의 모리스 웜과 2001년 발생한 슬래머 웜 모두 버퍼 오버플로를 발생하였으며, 다음 희생자를 찾기 위한 코드를 실행하기 위하여 command shell을 spawn한다. 이러한 사실로부터, 연결을 수락하거나 출력 연결을 만들기를 시도하는 command shell을 spawn하는 어떠한 서비스도 허용되지 않아야 된다는 것을 알 수 있다. 이것이 전형적인 HIPS가 동작하는 방법의 핵심이다.

다른 HIPS 시스템은 관측 접근(observational approach)을 사용한다. 그 이론은 에이전트는 호스트 상에서 수행되며 모든 시스템 콜, registry 목록 및 서비스 통신을 관측한다는 것이다. 관측기간 후에, 에이전트는 실행 모드로 설정될 수 있고 관측된 행위 밖의 어떠한 call도 커널 레벨에서 kill된다. 이 방법은 전통적인 "strict deny unless otherwise allowed" 모델을 택하고 있다.[6]

또 다른 방법으로 하이브리드 접근이 있다. 여기서 공격을 탐지하기 위하여 규칙, 애플리케이션 행위 및 시그니처의 결합을 사용한다. 이런 형태 시스템의 주요한 장점은 전에 보았든 혹은 시그니처가 존재하는 이름에 의하여 공격을 절대적으로 식별할 수 있는 능력에 있다.

Ⅳ. ITU-T X.805의 적용

ITU-T X.805 권고안은 종단간 네트워크 보안을 제공하기 위하여 네트워크 보안 구조를 정의한다. 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.[11] 이 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 BcN 관점에 적용될 수 있다.

〔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	

4.1 보안 디멘전

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

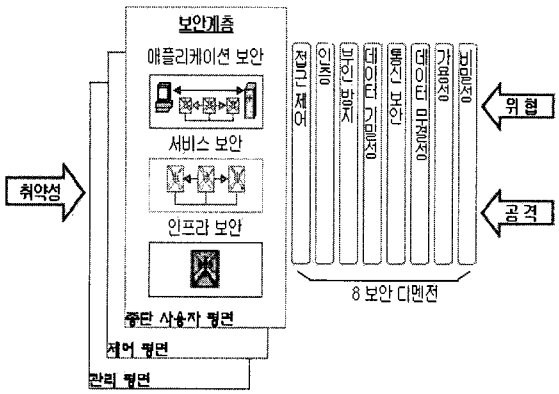
- 접근 제어: 네트워크 자원의 불법적인 사용에 대하여 보호하며, 단지 권한이 부여된 사람이나 장치만이 네트워크 요소, 저장 정보, 정보 플로, 서비스 및 애플리케이션에 접근이 허용되도록 보증한다. 예를 들어, 역할-기반 접근 제어(RBAC: Role-Based Access Control) 등이 있다.
- 인증: 통신 엔티티의 신원을 확인하며, 통신에 참여하는 엔티티의 신원의 정당성을 보증하고 엔티티가 가장공격이나 재생 공격을 시도하지 못하도록 한다.
- (송수신) 부인방지: 개인이나 엔티티가 데이터에 관련하여 특정 행동을 수행한 것을 부인하지 못하도록 하는 수단을 제공한다. 이는 책무, 의향 혹은 실행의 증명, 데이터 기원의 증명, 소유권의 증명, 자원 사용의 증명 등과 같은 네트워크-관련 행동의 이용 가능한 증명을 통하여 이루어진다.
- 데이터 기밀성: 데이터를 불법적인 노출로부터 보호하며, 데이터의 내용을 권한이 부여되지 않은 엔티티가 알지 못하도록 보증한다. 이를 위한 방법으로는 암호화, 접근제어 목록(ACL: Access Control List) 등이 있다.
- 통신 보안: 정보 플로가 단지 권한이 부여된 종단점 사이에서만 이루어지도록 하며, 정보가 다른 곳으로 전환되거나 포획되지 않도록 한다.
- 데이터 무결성: 데이터의 정확성을 보증하며, 불법적인 변조, 삭제, 생성, 복제로부터 보호한다.
- 가용성: 네트워크에 영향을 미치는 이벤트로 인하여 네트워크 요소, 저장 정보, 정보 플로, 서비스 및 애플리케이션에 대하여 권한이 부여된 접근 거부가 없도록 보증한다.
- 비밀성: 네트워크 행위의 관측으로부터 유도될 수 있는 정보 보호를 제공한다. 이 정보의 예로는 사용자 방문 웹 사이트, 사용자의 위치, 서비스 제공자 네트워크 안의 장치 IP 주소 및 DNS 이름 등이 있다.

4.2 보안 구조

그림 1은 종단간 네트워크 보안을 위한 보안 구조를 보여준다. 종단간 보안 솔루션을 제공하기 위하여, 4.1절에서 기술된 보안 디멘전이 각 보안 계층에 적용되어야 한다. X.805는 세 개의 보안 계층을 정의한다.

- 인프라 보안 계층
- 서비스 보안 계층
- 애플리케이션 보안 계층

보안 계층은 네트워크 보안의 순차적인 관점을 제



〔그림 1〕 종단간 네트워크 보안을 위한 보안 구조[11]

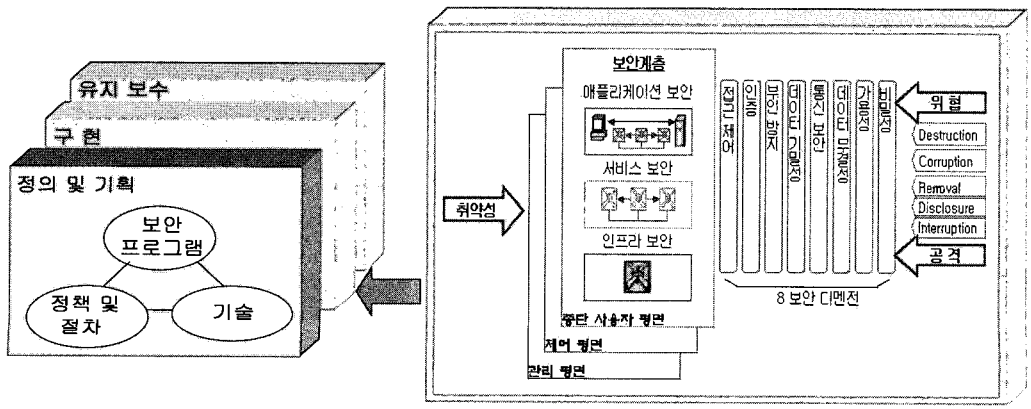
공함으로써 제품과 솔루션의 어디에서 보안이 다루어져야 하는가를 식별한다. 예를 들어, 최초의 보안 취약성이 인프라 계층을 위하여, 다음에 서비스 계층을 위하여 다루어지고, 마지막으로 보안 취약성이 애플리케이션 계층을 위하여 다루어진다. 그림 1은 각 계층에 존재하는 취약성을 감소시키고 그리하여 보안 공격을 완화시키기 위하여 어떻게 보안 디멘전이 보안 계층에 적용되는지를 보여준다.

각 계층의 기능은 아래와 같다.

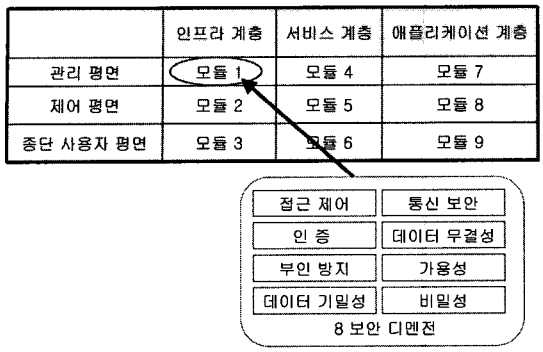
- 인프라 보안 계층: 보안 디멘전에 의하여 보호되는 개별 네트워크 요소뿐만 아니라 네트워크 전송 설비로 구성된다. 이 계층에 속하는 컴포넌트의 예로 개별 라우터, 교환기, 서버 및 통신 링크 등이 있다.
- 서비스 보안 계층: 서비스 제공자가 고객에게 제공하는 서비스의 보안을 다룬다. 기본 전송 및 연결 서비스로부터 부가 가치 서비스에 이르는 여러 가지 형태의 서비스가 있다. 이에 대한 예로는 AAA 서비스, 도메인 네임 서비스, QoS, VPN 등이 있다.
- 애플리케이션 보안 계층: 접근되는 네트워크-기반 애플리케이션의 보안을 다룬다.

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 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



〔그림 2〕 보안 프로그램에 대한 보안 구조의 적용[11]



〔그림 3〕 표 형태의 보안 구조[11]

계층에 적용되는 8개의 보안 디멘전을 결합한다.

V. Secure QoS

5.1 QoS 공격 목표

BcN에서 QoS를 신뢰성있게 제공하기 위하여 QoS 구조에서 보안 개념이 도입되어야 한다. QoS 공격에 대한 목표는 다음과 같은 것이 있다.

- 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: 특정 사용자의 원래 예약 요구와 아주 다른 자원을 공격자가 예약하도록 할 수 있다.
- 네트워크 이용 저하: 네트워크 시스템이 어떤 QoS 요구사항의 집합을 지원할 수 있을 만큼 충분한 자원을 가지고 있더라도, 네트워크가 작은 부분집합만을 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.

5.2 문제점

앞에서 기술한 바와 같이 보안은 본질적으로 단일 차원이 아닌 많은 속성들, 즉, 기밀성, 무결성, 가용성으로 구성되어 있다. 이 세 개의 속성들은 하부 시스템이나 통신 채널들의 다른, 많은 경우 모순된 요구사항을 기술한다. 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 척도로 간주되어야 한다.[12]

따라서 QoS 구조에 포함될 다른 보안 측면을 위한 정량적인 값에 이르기 위한 방법을 정의하여야 한다. Irvine [13]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. 대부분 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"(security parameter)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 암호법에 대한 한 가지 예는 다음과 같다.

평문 ≤ DES ≤ AES

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

5.3 RSVP 보안

5.3.1 QoS 메커니즘과 공격자 분류

본 절에서는 RSVP 보안을 기술하기 위하여 필요

한 RSVP에서의 QoS 메커니즘에 대하여 간략히 기술한다.[14] 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.

[14]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.[11] $Insider_{RSVP} \geq Outsider_{OnPATH} \geq Outsider_{Other}$

5.3.2 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.

4) 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.

5) 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.

6) 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.

5.3.3 대응 방법

IETF/RSVP의 보안 솔루션인 홉별 인증은 $Outsider_{OnPATH}$를 방지하는 데만 유용하며, 어떤 $Insider_{RSVP}$ 공격을 다룰 수 없다. $Insider_{RSVP}$ 공격을 다루기 위하여 [14]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 것

이다. 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.

5.4 DiffServ 보안[15]

5.4.1 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 SLA에 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.

5.4.2 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 수

행할 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.

5.4.3 제안된 솔루션

이러한 잠재적인 보안 관심사의 결과로, IETF 워킹 그룹은 여러 가지 방법을 제안하였다. 본 논문에서는 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.

5.5 MPLS 보안[16]

5.5.1 요구사항

이 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.[16] 만일 네트워크가 안전하지 않은 경우, MPLS 하부구조 상에 IPSec을 수행할 필요가 있다. 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 동일한 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 제공하는 침입 공격에 대하여 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.

5.5.2 분석

본 절에서는 앞 절에서 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 다른 VPN이나 인터넷으로부터의 DoS 공격에 대하여 구조를 개방할 수 있기 때문이다.

[16]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.

5.5.3 보완점

[16]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.

Ⅵ. 보안 SLA

서비스수준협약(SLAs: Service Level Agreements)은 보장된 품질 수준과 관련되는 메트릭(metric)을 상술하는 서비스 제공자와 고객들 사이의 공식적인 계약이다. BcN에서 일반적 SLA는 대역폭, 지연, 손실, 지터 같은 메트릭과 그들의 보장된 수준을 나타낸다. 서비스 제공자에 의하여 구현되는 SLA는 측정될 수 있고 추적될 수 있는 메트릭에 기초한다. 그러한 메트릭으로 서비스 제공자뿐만 아니라 고객들도 잘 이해하고 있는 서비스 가용성(availability)이 있다. 예를 들어 BcN의 서비스 가용도가 99.999%일 때 1년에 접속 불량 시간 10분 이내의 품질 서비스 제공이 가능하여 진다.

그러나, 보안 서비스에 대한 SLA의 개념은 상대적으로 새로우며, 메트릭이 잘 확립되지 않았다. 정보통신 인프라의 보호에 대한 관심이 증대하여 짐에 따라, 네트워크를 안전하게 하고 재앙으로부터 복구할 수 있

는 메커니즘으로 어떻게 보안 SLA가 사용될 수 있는지를 조사할 필요가 있다. 그러면 보안 SLA의 내용은 어떤 것이 있는지 기술한다.[17] 먼저 보안 SLA의 범주를 물리적 보안과 사이버 보안으로 나눌 수 있다. 물리적 보안은 중요한 자원에 대한 물리적인 보호를 의미하고, 본 논문에서는 다루지 않는다. 사이버 보안은 사이버 공격과 연관되어 발생되는 경감 및 서비스 복구 문제를 다룬다.

ITU-T X.805 권고안은 통신망을 위한 종단간 보안 프레임워크를 기술하고 있다. 이 권고안에서 종단간 네트워크 보안을 위한 보안구조를 보여주는데, 8개의 보안 디멘전이 보안 SLA 속성으로 잠정적으로 사용가능하다. 이 속성을 이용하여 가능한 보안 속성과 SLA 사양은 표 2와 같다.

보안 SLA는 네트워크의 특정한, 미리 정해진 경계(boundary)와 조건 안에서 유효하다. SLA 경계는 유효한 사용자 시나리오 하에서 다른 서비스 특징들에 대한 트래픽 플로우를 기술하는 참조 연결을 서류화함으로써 식별된다. 참조 연결은 트래픽과 애플리케이션 클래스의 보안 요구사항을 또한 기술한다. 보안 SLA를 기술하기 위하여 사용되는 참조 연결은 어떻게 이런 보안 요구사항들이 구현되는지와 제한 사항에 대한 상세한 내용을 제공해야 한다. 서비스 제공자는 VPN과 인터넷 액세스 서비스를 제공하기 위하여 공통의 인프라 요소를 사용한다. 다른 보안 SLA들은 라우팅, 보안과 서비스 품질 설계에 의하여 공통 공유 인프라 상에서 여전히 성취될 수 있다. 위에서 기술된 바와 같이 보안 구조와 참조 연결들을 서류화함으로써 SLA 척도에 영향을 주는 네트워크 자원들을 식별할 것이다. SLA의 보안 구조 서류화에 포함되어야 할 항목들의 예는 아래와 같다.[17]

- 네트워크, 서비스, 애플리케이션을 위한 보안 요구사항
- 시그널링, 사용자 데이터 전달, 관리를 위한 프로토콜
- 보안 기술(방화벽, 필터, 침입탐지시스템, 로그 파일, 싱글 사인온, 인증 방법)

(표 2) ITU-T X.805 권고안의 보안 디멘전에 대한 확장: 보안 SLA[17]

SLA 속성	보안 목적 요약	SLA 예	척도 예
접근 제어	권한이 부여된 사람이나 장비만 접근 허용	99% 허용된 접근	- 인증 메커니즘이 구현된 장비의 비율 - 오 거부(false denial) 비율 - sys 로그, 방화벽 로그 분석에서 비권한 접근 비율
인증	신원 검증	1 factor 인증 이상의 99% 사용	- 인증을 요구하는 자원 % - 비인증된 접근 허용 시간 % - 안전한 인증 방법 사용 시간 %
부인 방지	행위에 대한 기록 제공	99%가 부인방지 메커니즘 사용	- 디지털 서명 사용 % - 인증 당국 활성 시간 % - 상호관련된 일별 감사 로그
데이터 기밀성	데이터 공개 보호	99%의 시간에 암호화 응용 지원	- 강건한 암호화 사용 응용 % - 안전한 키 교환 시간 %
통신 보안	정당한 정보 흐름 보증	장비의 99%가 통신당 보안 기술 지원	- 세션이 하이잭 당한 시간 % - 성공적으로 완료된 트랜잭션 % - 일별 거래 로그 보고서
데이터 무결성	데이터 정확성, 변경 보호	무결성을 지원하는 네트워크 단말의 비율	- 무결성 조사 결여로 인한 위반 탐지 혹은 공격 발생 % - 무결성 조사를 지원하지 않는 네트워크 장치 %
가용성	자원의 정당한 사용 보증	99%의 서비스 가용성과 MTTP (mean time to patch)	- DoS 혹은 DDoS로 인한 다운시간 - 보안 패치 갱신으로 인한 다운 시간 - 비유효 인증으로 인한 다운 시간 - 웜/바이러스 공격으로 인한 다운 시간 - 장비 실패로 인한 다운 시간
비밀성	정보 노출 방지	- 안전한 응용을 위한 각 계층의 비밀성 구현 비율 - 피어 대 피어 보안을 지원하는 장비 %	- 위장 공격 발생 시간 % - IPv6의 침투 % - 사용자 프로파일 보호나 수정을 위하여 사용되는 암호화 방법 - 사용자 프로파일에 대한 접근을 요구하는 거래의 %

· 수락 가능한 사용자 정책을 포함하는 보안 정책
· 보안 측정의 표준화

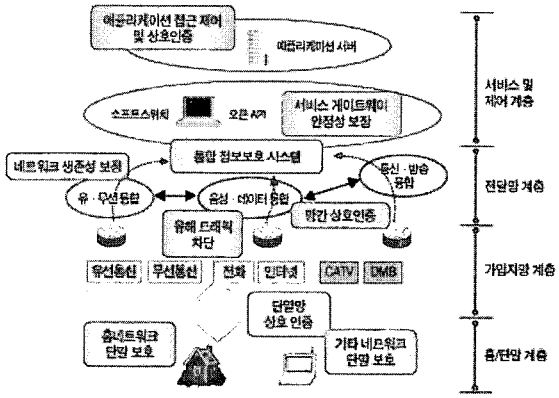
보안 SLA는 설계 요구사항, 산업 최선 실제와 적용 가능한 표준에 대한 일치성 정도를 기초로 평가될 수 있다. SLA를 보장하는데 있어서 척도의 역할에 대하여 알아볼 필요가 있다. 가용성과 인증을 위한 척도는 정지(outage)와 다운시간에 대한 네트워크 통계치를 사용하여 측정되고 추적될 수 있다. 따라서 이 두 개의 보안 디멘전을 위한 SLA를 확립하는 것은 전통적인 SLA 프로세스를 따를 것이다. 비밀성, 무결성, 데이터 기밀성과 통신 보안을 위한 SLA 척도도 서비스와 인프라 보안을 위하여 또한 중요하다. 통신 보안은 참조 연결 내에 나열된 요구사항과 일치하여 성공적으로 완료된 거래의 백분율을 나타내는 척도로 추적될 수 있다. 이 척도의 일치성 감시는 원격 액세스 프로토콜의 보안, 애플리케이션과 네트워크 요소 안의 다른 보안 구현에 의존한다.

Ⅷ. BcN 보안 기능 고도화 방안

BcN 환경에서는 보안 침해 사고가 발생하면 그 피해가 전체 네트워크로 광범위하게 확산되어 심각한 통신 피해가 우려되고, 또한 통신망의 기능이 다양화되고 고도화될수록 관련 침해 대응 기술의 고도화도 요구된다. 이에 따라 국내에서도 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 연동할 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 3은 단계별 보안기능 고도화 방안을 보여준다. 표 3에 의하면, 1단계에서는 DDoS 및 웜 해킹 대응, 과다 트래픽 감시, 홈네트워크 단말 보호 등의 기술이 개발될 예정이며, 수 Giga 급 보안장비가 BcN 전달망에



(그림 4) BcN 보안망 체계도[1]

(표 3) 단계별 보안기능 고도화 방안[1]

구분	상호인증 및 접근제어	네트워크 생존성 보장	BcN 시스템 보호
1단계 (2004~05)	- 단말·망상호인증 - 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 보안관리 시스템	- 통신·방송 융합형 단말 보호 - BcN 노드 보안

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
- ·정보보호 법·제도 개선

Ⅷ. 맺음말

BcN 전달망의 특징은 QoS 보장, 보안 기능 제공, IPv6 수용, 개방형 망 구조로 요약할 수 있다. BcN 환경에서는 보안사고 발생 시에 그 피해가 전체적인 정보통신 인프라에 보다 빠르게 광범위하게 확산될 수 있기 때문에 더욱 심각한 통신 피해가 우려되고, 따라서 BcN을 위한 보안 대책이 적절히 수립되어야 한다.

그러나 국내에서 아직 BcN의 보안 관련 기술에 대한 참고문헌이 거의 없는 실정이다. 따라서 본 논문에서는 BcN 보안 취약성과 요구사항에 대하여 살펴보고, BcN 인프라 보호 기술, 광대역 통합망 관점의 보안 구조 개발에 적용될 수 있는 ITU-T X.805에 대하여 살펴보고, 또한 QoS 구조에서 보안 메커니즘을 도입하기 위한 문제점과 방안에 대하여 기술하였다. 보안의 중요성이 증가함에 따라, BcN을 위한 SLA에 ITU-T X.805에서 기술된 보안 디멘전을 위한 보안-형태의 메트릭이 보충되어야 한다. 또한 일치성 형태의 메트릭도 포함될 필요가 있다. 이에 따라 보안 SLA의 개념에 대하여도 기술하였다. 마지막으로 국내에서 추진되고 있는 BcN 보안 기능 고도화 방안에 대하여 기술하였다.

향후 안전한 광대역 통합망의 구현을 위하여 BcN에 관련된 보안 기술의 연구개발이 체계적으로 추진될 필요가 있다고 생각된다.

참 고 문 헌

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

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

[3] "Telecommunications and Internet Protocol Harmonization over Networks(TIPHON) Security: Threat Analysis", DTR/TIPHON - 08002 V0.1.9 (2001-02-09).

[4] 서동일, 김광식, 장종수, 손승원, "IT 839 전략 추진을 위한 정보보호 기술개발 방향", 한국전자통신연구원 전자통신동향분석 제 20권 제 1호, 2005년 2월.

[5] Carl Endorf, Eugene Schultz, and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004.

[6] Eric Ahlm, Is Intrusion Prevention Changing Information Security?, Rev. Ver. 1.1, March 2004, Vigilar Inc..

[7] A White Paper by NetScreen Technologies Inc., Intrusion Detection and Prevention: Protecting your network from attacks, version 2.0, http://www.netscreen.com

[8] Ian Poynter and Brad Doctor, Beyond the firewall: The next level of network security, StillSecure, Jan. 2003.

[9] Top Layer White Paper, Beyond IDS: Essentials of Network Intrusion Prevention, pp.1-18, Nov. 2002.

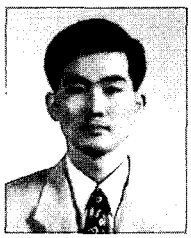
[10] Neil Desai, Intrusion Prevention Sys-

tems: the Next Step in the Evolution of IDS, http://www.securityfocus.com/printable/infocus/1670, Feb. 2003.
[11] ITU-T X.805 Rec., Security architecture for systems providing end-to-end communications.
[12] Stefan Lindskog, Erland Jonsson, "Introducing Security in QoS Architectures", http://www.ida.his.se/ida/conf/PromoteIT2002/5D3LindskogStefan.pdf.
[13] 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, pp. 334-343, New Orleans, Louisiana, USA, Dec. 11-15, 2000.
[14] Tsung-Li Wu, S. Felix Wu, Zhi Fu, He Huang, Feng-Min Gong, "Securing QoS: Threats to RSVP Messages and their Countermeasures", http://citeseer.ist.psu.edu/wu99securing.html.
[15] A. Striegel, "Security Issues in a Differentiated Services Internet", http://www.ee.iastate.edu/~gmani/tiw-2002/diffserv-security.pdf .
[16] Cisco Systems, White Papers, Security of the MPLS Architecture, Cisco Systems Inc.
[17] Chun K. Chan, Uma Chandrashekhar, Steven H. Richman, and S. Rao Vasireddy, "The Role of SLAs in Reducing Vulnerabilities and Recovering from Disasters", Bell Labs Tech. Journal, 9(2), pp.189-203, 2004.

〈著 者 紹 介〉

전 용 희(Yong-Hee Jeon)
종신회원

1971년 3월~1978년 2월 : 고려대학교 전기공학과
1985년 8월~1987년 8월 : 미국 플로리다공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월 : 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월 : 삼성중공업(주)
1978년 11월~1985년 7월 : 한국전력기술(주)
1979년 6월~1980년 6월 : 벨기에 Belgatom 연수
1989년 1월~1989년 6월 : 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월 : 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월 : 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재 : 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년 3월~2003년 2월 : 대구가톨릭대학교 공과대학장 역임
2004년 2월~2005년 2월 : 한국전자통신연구원 정보보호연구단 초빙연구원
〈관심분야〉 네트워크 보안, BcN QoS & Security, 통신망 성능분석



장 종 수 (Jong Soo Jang)
정회원

1984년 : 경북대학교 전자공학과 공학사
1986년 : 경북대학교 전자공학과 공학석사
2000년 : 충북대학교 컴퓨터공학과 공학박사
1989년 ~현재 : 한국전자통신연구원 정보보호연구단 네트워크보안그룹 그룹장
〈관심분야〉 네트워크보안, 웹서비스보안, Secure OS, IDS/IPS, Traffic Management