주 제

BcN 보안 기술 및 표준화 동향

대구가톨릭대학교 **전용희**

차 례

I. 서 론

광대역 통합망(BcN : Broadband convergence Network)이란 통신 · 방송 · 인터넷이 융합된 품질 보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊어짐 없이 안전하게 광대역으로 이용할 수 있는 차세대 통합네트워크로 품질(QoS: Quality of Service) 보장망과 통합(Convergence)망의 두 가지 특성으로 정의된다. 품질보장망이란 종단간(End-to-End) 구간에 대한 이용자별 QoS 요구사항을 만족시키는 음성 데이터 통합, 유무선 통합 및 통신방송 융합 서비스를 제공할 수 있는 통신망이다. 통합망이란 전화망, 인터넷망, 이동통신망, 전용회선망, 방송망 등의 백본 네트워크를 통합하여 궁극적으로 유,무선 방송 서비스의 융합서비스를 제공하고 더 나아가 통신과 정보의 종합 객체가 되는 유비쿼터스 환경을 제공하기 위한 통신망이다[9]. 다른 형태의 전송 구조를 고려하여, BcN에서 발생할 수 있는 주요한 위협의 형태로는 다음과 같은 것이 있다[6].

- 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.

본 논문에서는 먼저 BcN 보안의 필요성 및 보안 기술에 대하여 알아보고, ITU-T에서 완료된 종단간 통신을 위한 보안 구조인 ITU-T X.805의 내용에 대하여 기술하고, 이를 기반으로 설정되고 있는 ITU-T NGN 보안 기반구조 및 보안 요구사항에 대하여 제시한다. 마지막으로 BcN 보안과 관련한 국내 표준화 추진 동향 및 계획에 대하여 기술하고자 한다.

II. BcN 보안의 필요성

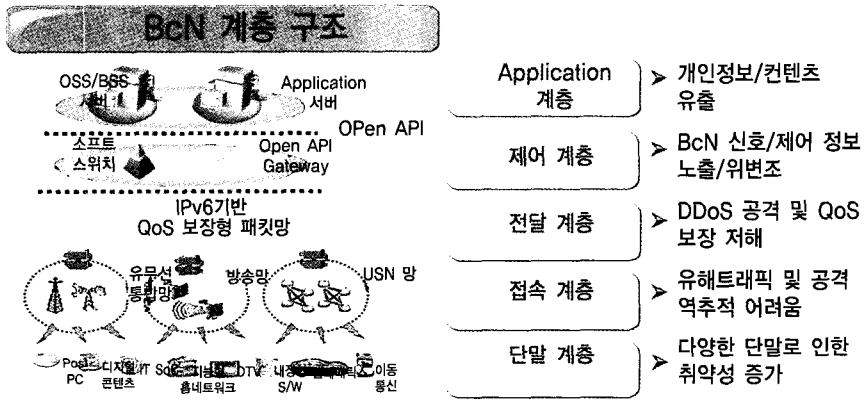
BcN은 개방형 망구조(Open API)의 지원으로 다양한 경로를 통하여 통신망에 대한 접근이 쉬워지고, 이를 이용한 해킹 공격 및 바이러스 유포 등의 위험성이 존재한다. BcN에서 고려되어야 할 위협요소는 다음과 같다[3,5,6,8].

- 개별 통신망에 대한 위협이 전체 통신망으로 확산될 가능성이 더욱 높아진다. 이것은 개별 통신망들이 상호 통합되기 때문에 기존의 개별적인 통신망에 대한 피해가 BcN으로 연결된 음성통신망, 방송망, USN(Ubiquitous Sensor Network)까지 모든 구성 네트워크로 그 피해가 확산될 수 있기 때문이다. 따라서 대응 방법도 그에 따라 달라져야 한다. 현재의 네트워크 보안은 소규모 네트워크 차원에서 이루어지는 단순한 형태의 모니터링 및 보안 정책을 적용하나, BcN 환경에서는 네트워크 전체에 대하여 체계적으로 통합 관리함으로써 신속한 대응 체계를 갖출 필요가 있다.
- 네트워크 대역폭의 증가로 전송 속도가 빨라져 웜과 같은 악성 코드의 확산을 가속화 시킬 수 있다. 그러므로 네트워크 공격에 대하여 대응할 수 있는 시간도 단축된다. 이에 따라 Zero-day 공격에 대응할 수 있는 No Signature IPS (Intrusion Prevention System) 등에 대한 기술 개발이 요구된다.
- IPv6 기반의 BcN에서 IPv6 기능의 취약점을 이용한 새로운 공격이 발생될 가능성이 있다. 따라서 IPv4망에서 발생되었던 여러 가지 기존의 위협 형태를 포함하여 새롭게 IPv6에서 발생될 수 있는 취약점, 기존 IPv4에서 IPv6로 전환하는 단계에서 발생할 수 있는 위협이 있다.
- BcN과 연결되는 USN에서의 취약점이 있다. 사용되는 CPU 용량이 적고 저전력을 사용하기 때문에 자원에 대한 DoS 공격에 취약하고, 분산되어 설치된 센서를 통한 개인정보보호 침해에 대한 문제가 발생할 수 있다.

네트워크 혹은 서비스 제공자는 위협 분석과 위험 평가의 결과를 근거로, 어떤 보안 대책을 수립할 것인지를 결정해야 한다. (그림 1)은 BcN 계층별 정보보호 위협을 보여준다[7].

(그림 1)의 BcN 정보보호 위협에 대하여 좀 더 자세히 기술하면 다음과 같다.

- 개방형 인터페이스를 사용하는 어플리케이션 계층의 사용자 개인정보 및 개방형 서비스 구조에서 제공되는 컨텐츠에 대한 지적 재산권 침해 위협



(그림 1) BcN 계층별 정보보호 위협

- 과금, 인증, 정책, 설정정보와 등과 같은 중요 제어/설정 정보의 노출 · 위변조 및 OSA(Open Service Access) Gateway, 소프트스위치 등 BcN의 중요 시스템에 대한 침해 위협
- 악의적인 제어 메시지 배포를 통한 불법적인 대역폭 사용, 타인의 대역폭 조정 등을 통한 서비스 품질 저해 및 과다 트래픽 발생을 통한 DoS 및 DDoS 공격에 대한 위협
- 이동성이 보장되고 다양한 접속망이 제공되는 환경에서 복수의 접속기술이 통합된 복합단말기를 통한 공격의 역추적 어려움과 다양한 단말로부터의 유해트래픽 유입에 대한 위험 증가
- 인터넷 침해사고에 취약한 인터넷망에서 발생된 위협이 BcN을 통해 통신망, 방송망 및 USN까지 확산 가능

위에서 기술한 BcN 정보보호 위협은 아래와 같은 계층별 취약점과 관련된다[3].

- 홈/단말 계층: 홈 게이트웨이 안정성, 가입자 망 접속 장비의 정보보호, 이동성 보장에 따른 공격자 역추적의 어려움, 위장 단말기 탐지
- 접속 계층: 망 통합으로 인한 취약성 확산, 악의적 공격의 위치 다양화 및 역추적 문제, 비인가 접속 차단, 도청 · 데이터 위변조
- 전달 계층: DDoS 공격 등으로 인한 BcN 생존성, QoS 보장, 이종망간 상호 연동 시 정보보호
- 제어 계층: BcN 관리/제어 정보 보호, 서비스 게이트웨이 및 소프트스위치 신뢰성 보장
- 어플리케이션 계층: 접근 인증 및 권한, Open API 제공, 사용자의 개인정보 보호, 불건전 정보 유통

이와 같이 정보통신망 기능의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 제반 위협과 부작용 등의 정보화 역기능에 대한 대응을 위하여 BcN 정보보호가 필요하다. BcN에서는 이기종 망간 통합 및 여러 사업자간에 연동이 이루어지기 때문에 체계적으로 침해사고에 대처하기 위하여 통합 정보보호 관리체계의 구축이 필요하고, 사이버 공격이 갈수록 지능화 · 다양화 · 고속화되는 상황에서 개별망의 피해가 다른 망으로 확산될 수 있는 환경에 대응할 수 있도록 침해사고 예방 및 대응체계에 대

한 고도화가 필요하다. 아울러 사용자 프라이버스 보호를 위한 사전 진단 및 지침에 대한 마련이 필요하고, BcN 환경에서 사용될 수 있는 고성능/QoS-aware 네트워크 정보보호 기술이 개발되어야 한다. 또한 정보보호 안정성이 검증되지 않은 VoIP, 텔레매틱스 등 신규 서비스와 다양한 복합단말기에 대한 정보보호 기술이 개발되어야 하고, 신규 IT 서비스의 안정성 확보를 위한 정책적인 지원도 필요하다.

III. BcN 보안 기술

BcN 환경에서는 통신 · 방송 · 인터넷이 융합되어 다양한 콘텐츠와 서비스를 제공하는 통합망으로 설치되기 때문에 네트워크 공격의 위험성이 더욱 높아지고 취약성도 증가한다. 본 장에서는 BcN 보안을 위하여 필요하다고 생각되는 보안 기술들을 최근 기술동향을 고려하여 알아본다[1]. 국내에서 BcN 보안을 위하여 개발하고자 하는 기술에 대하여는 6장을 참고할 수 있다.

1. 콘텐츠 보안 기술

웹 서비스, 전자메일, P2P, 인스턴트 메시지 등과 같은 다양한 서비스 정보에 유해 및 불법 정보를 많이 포함하고 있는 Phishing 및 Pharming, 스팸(Spam), 악성 코드, 사회공학 등의 공격이 증가하고 있다. 이런 공격에 대응하기 위하여 콘텐츠 기반 보안 기술이 필요하다.

2. 침입 탐지/방지 기술

기존의 침입탐지시스템(IDS : Intrusion Detection System)의 단점을 보완하여 침입방지시스템(IPS: Intrusion Prevention System)이 개발되었다. IPS는 IDS가 지니고 있는 시그너처 기반에 유해 트래픽을 차단하는 기능을 추가한 기술이 제공되었는데, 이는 급속하게 증가하는 웜 트래픽에 대한 시그너처 생성에 소요되는 시간과 비용 문제, 네트워크 성능저하, 오탐율(False Positive) 문제를 가지고 있다.

3. 웜 봉쇄 기술

BcN에서의 웜의 확산을 방지하기 위하여 봉쇄(containment) 혹은 격리(quarantine) 기술이 개발되고 있다. 봉쇄는 활성 웜의 확산을 지연시키거나 방지하기 위하여 사용되는 메커니즘을 뜻한다. 현재 사용 중인 봉쇄 기법의 종류로는 세 가지가 있다.

• 호스트 격리(host quarantine)

호스트 격리는 감염 호스트가 다른 호스트와 통신하는 것을 단순히 막는 행동으로, 라우터나 방화벽 상의 IP-레벨 접근 제어 목록을 통하여 보통 구현된다.

• 스트링 매칭

스트링-매칭 봉쇄는 시그너처-기반 네트워크 침입방지시스템에서 대표적으로 사용하며, 네트워크 트래픽을 알려진 웜의 특정 스트링이나 시그너처와 매치하여 관련 패킷들을 탈락시킬 수 있다. 고속 매칭을 위하여 FPGA-기반 하드웨어 시스템이 개발되고 있다[4].

• 연결 throttling

연결 throttling 방법은 웜의 확산을 막는 것이 아니라, 지연시키기 위하여 외부 연결의 rate를 제한하는 기술이다. 이 기술에 대하여는 3.4에서 좀 더 기술한다.

웜의 봉쇄를 위하여 개발되고 있는 주요 시스템은 다음과 같다[19].

• Earlybird 시스템

콘텐트 유포를 탐지하기 위하여 콘텐트-감별(content-sifting) 접근을 사용한다. 주소 확산을 평가하기 위하여 기존 알고리즘 보다 훨씬 적은 메모리를 사용하여 정확하게 평가하는 눈금 비트맵(scaled bitmap)을 사용한다. 콘텐트 유포는 잠재적인 웜 시그너처 식별을 위한 주요 측정기준이고, 주소 확산은 이 집합에서 오탐율(false positive)을 줄이기 위하여 중요한 것이다. 센서가 구성 가능한 주소 공간 지역상의 트래픽을 감별하여 집합기(aggregator)에게 시그너처를 보고한다. 집합기는 센서들로부터의 실시간-갱신을 조정하며, 관련 시그너처들을 합병하고, 네트워크 혹은 호스트-레벨 차단(blocking) 서비스를 활성화한다.

• Autograph 기법

오토그라프[15]는 TCP 전송 프로토콜을 사용하여 전파되는 웜으로부터 시그너처를 자동으로 생성하는 시스템이다. 이 시스템은 부분적인 플로 페이로드의 유포를 분석하여 높은 민감성(sensitivity, 즉 true positive)과 낮은 특정성(specificity, 즉 false positive)을 나타내는 시그너처를 생성한다. 콘텐트 유포 분석 수행을 위한 트래픽 양을 감소하기 위하여 포트-스캔-기반 플로 분류기를 사용한다. 오토그라프는 분산 배치를 위하여 보다 나은 지원을 하며, 분산 모니터 사이에 포트-스캔 보고를 공유하기 위하여 애플리케이션-레벨 멀티캐스트를 사용한다.

• TRW(Threshold Random Walk) 알고리즘

[20]에서는 TRW 온라인 악성-호스트 탐지 알고리즘을 기반으로 하는 스캔 탐지 및 억압(suppression) 알고리즘을 개발하였다. 알고리즘의 단순화로 하드웨어 및 소프트웨어 구현에 적합하도록 하였다. 주소 별 및 개별 연결들의 활동을 추적하기 위하여 캐시를 사용한다.

봉쇄 장치 사이에서 협동(cooperation)을 통하여 봉쇄를 증진시킨다. 통신을 통하여 경계치(threshold)를 감염 수준까지 동적으로 조정할 수 있다. 웜 봉쇄 시스템들은 감염 경계치(epidemic threshold)를 가진다. 만약 취약 머신의 수가 특정한 봉쇄 배치에 비하여 충분히 적으면, 봉쇄가 웜을 거의 완벽하게 정지시킬 것이다.

• 기타

기타 웜의 봉쇄 기술로 동향 탐지(trend detection)라고 하는 웹 모니터링 및 조기 경보 시스템[10], 자동 시그너처 생성과 분류를 가진 고속 웜 탐지를 위한 DHT(distributed hash table)-기반 오버레이 시스템을 이용하는 NetShield 시스템[19], 네트워크 트래픽 분석 대신에 취약 호스트가 감염되는 것을 방지하기 위하여 종단-시스템 접근을 채용한 웜 백신 프로젝트[22]와 Microsoft의 Shield 시스템[14]이 있다. Symantec 등에서도 조기-경보 및 모니터링 시스템과 웜 봉쇄 기술에 대하여 연구를 진행하고 있다.

4. Rate-Limiting 기술

이 기술은 자동 대응 기법의 한 종류로, 합법적인 애플리케이션의 지속적인 운용은 허용하면서 웜 트래픽의 외부 확산을 rate limit하는 방법이다. 최근의 분석 연구는 rate limiting이 네트워크에서 적절한 지점에 배치되면 감염 확산을 상당부분 감소할 수 있다는 것을 보여준다[11,12]

Rate limiting 기법으로 다음과 같은 것이 있다.

• IP throttling [18]

Throttling 기법은 활동 집합 안에 있는 주소들을 위한 외부(outgoing) 연결은 허용하지만, 다른 패킷들은 지연 버퍼에 넣어 지연 시킨다. 만약 지연 버퍼가 차면, 추가적인 패킷들은 단순히 탈락된다. 지연 버퍼에 들어 있는 패킷들은 일정한 율로 처리된다. 같은 율로 활동 집합 안의 가장 적게 사용된 최근 주소는 새로운 연결을 위한 공간을 위하여 삭제된다. 결과적으로, 빈번히 사용되는 주소에 대한 연결은 높은 확률로 허용되고, 반면에 스캐닝 웜에 의하여 개시되는 임의 주소에 대한 연결은 지연되고, 이루어지지 않도록 하는 것이다.

• 실패-연결-기반 스킴 [21]

이 기법은 스캐닝 웜에 의하여 감염된 호스트가 많은 수의 실패 TCP 요구를 생성한다는 가정을 기반으로 한다. 이 기법은 이런 현상을 감염의 지시로 사용하며 그러한 행위를 가진 호스트를 rate limit 한다. FC(Failed Connection) 기법은 에지 라우터 기반으로 두 과정으로 구성된다.

처음 단계에서, 잠재적인 "감염" 호스트를 식별한다. 이 단계 동안 호스트에 대한 실패 통계를 저장하기 위하여 해시(hash) 테이블이 사용된다. 라우터에서 보관되는 호스트-별 상태의 양을 제한하기 위하여 심하게 경쟁하는 해시 테이블이 사용된다. 해시 테이블에서 한 항목에 대한 실패율이 어떤 경계를 초과하면, 알고리즘은 두 번째 단계로 들어간다. 이 단계에서 특정 해시 항목에서 호스트에 대한 rate limit를 시도한다.

• 크레디트-기반 [23]

CB(CB: Credit-based) 기법은 FC 기법과 두 가지 측면에서 상당히 다르다. 먼저 CB 기법은 첫 번째 연결 즉, 이전에 방문한 적이 없는 주소들에 대한 외부 연결에 대하여만 한정하여 rate limiting을 수행한다. 이것은 스캐닝 웜이 많은 양의 실패 연결을 생성하는데, 대부분 실패 일차-접촉 연결 수로 이루어진다는 관측을 바탕으로 한다. 따라서 비정상 일차-접촉 통계치가 rate limiting을 유발하는 스캐닝 행위의 표시이다. 일차 접촉 개념은 CB에 기본적이다. 두 번째로, CB는 실패와 성공 연결 통계치 모두를 고려한다. 간단히 말해서, CB는 호스트 당 어떤 수의 연결 크레디트를 할당한다. 각 실패 일차-연결은 한 개의 크레디트를 소모하며, 성공적인 일차 연결은 한 개를 추가한다. 호스트는 자신의 남은 크레디트가 양수일 때만 일차-접촉 연결이 허용된다.

• DNS-기반 [14]

DNS-기반 스킴은 웜 프로그램이 합법적인 애플리케이션과는 분명히 다른 DNS 통계치를 유발한다는 원칙에 기반을 두고 있다. 예를 들어, DNS 룩업이 존재하지 않는 것이 스캐닝 활동의 징표이기 때문이다. 이 관측은 Ganger [13]에 의하여 처음 행하여 졌다. [11]에 의하여 제안된 기법은 Ganger의 NIC-기반 DNS 탐지 기법의 변형이다.

DNS 기반 기법은 모든 출력 TCP SYN에 대하여, 목적지 IP에 대하여 이전의 DNS 번역이 존재하면 패킷을 통과시키고, 그렇지 않으면 SYN 패킷이 rate limit된다.

IV. ITU-T X.805 표준안

ITU-T X.805 권고안은 종단간 네트워크 보안을 제공하기 위하여 네트워크 보안 구조를 정의한다. 이 권고안은 2003년 9월에 ITU-T SG17에서 최종적으로 표준에 채택되었다. 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[16,17]. 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. ITU-T NGN FG(focus group)에서 이 보안 표준을 NGN을 위한 기본 보안 프레임워크 설정을 위한 기초 문서로 사용하고 있기 때문에, BcN을 위한 보안 관점에 또한 적용할 수 있을 것이다.

1. 보안 위협과 디멘전

ITU-T Rec. X.800에서 기술하고 있는 위협은 가용성에 대한 공격으로 정보와 다른 자원의 파괴, 정보와 다른 자원의 절도, 제거 혹은 손실, 서비스의 차단 등이 있으며, 무결성에 대한 공격으로 정보의 오손 혹은 변조, 기밀성에 대한 공격으로 정보의 노출 혹은 누설을 정의한다.

<표 1>은 보안 위협에 대한 보안 디멘전(security dimension)의 매핑(mapping)을 제공한다. 보안 디멘전은 앞에서 기술된 보안 위협에 대처하기 위한 보안 대책들의 집합인 보안서비스를 의미한다. 매핑은 각 보안 관점에 대해서 동일하다. 블록 안에 있는 Y자는 특정한 보안 위협이 해당 보안 디멘전에 의하여 대항한다는 것을 나타낸다. 8가지 종류의 보안 서비스가 정의되었으며, 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 개체의 신원을 확인하며, 통신에 참여하는 개체의 신원의 검증하고, 개체가 위장공격이나 재생 공격을 시도하지 못하도록 한다. 예를 들어, 비밀 공유, PKI(Public-Key Infrastructure), 디지털 서명 등이 있다.
- (송수신) 부인방지 : 개인이나 개체가 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 애플리케이션으로의 인가된 접근에 대한 서비스 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. 예를 들어, NAT와 암호가 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	

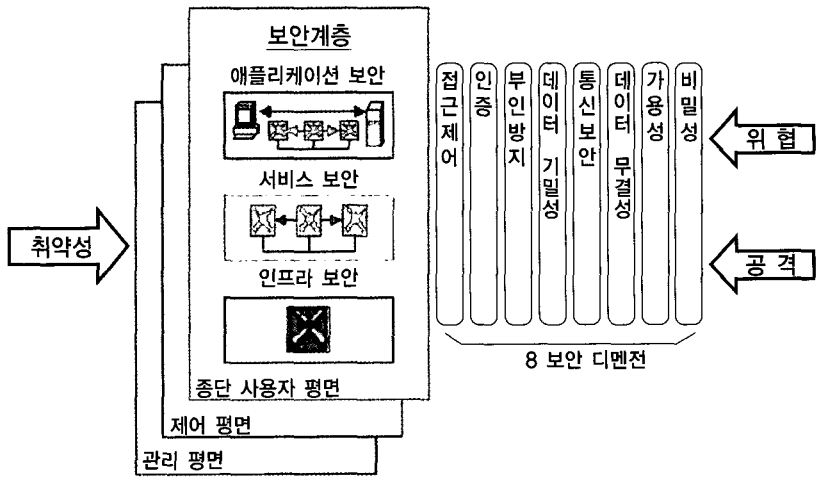
2. 보안 구조

(그림 2)는 종단간 네트워크 보안을 위한 보안 구조를 보여준다. 종단간 보안 솔루션을 제공하기 위하여, 4.1에서 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 제공함으로써 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 2)는 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,



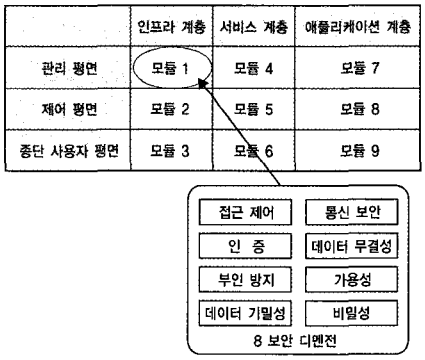
(그림 2) 종단간 네트워크 보안을 위한 보안 구조

VPN 등이 있다.

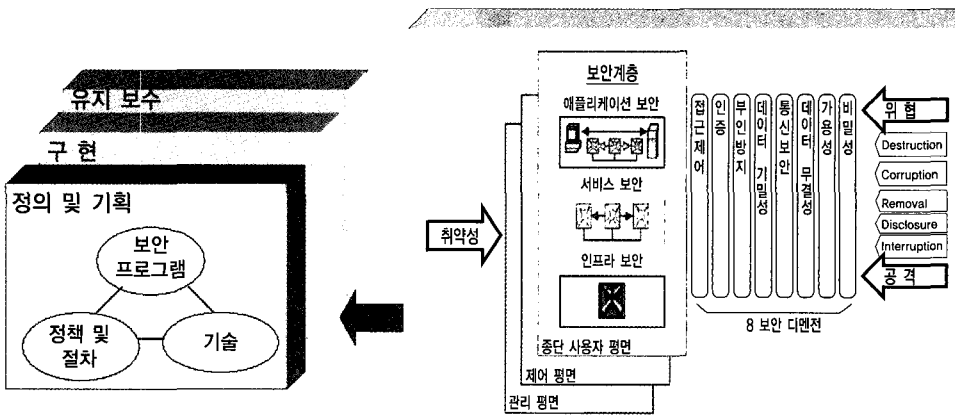
- 애플리케이션 보안 계층: 접근되는 네트워크-기반 애플리케이션의 보안을 다룬다.

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 3)은 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 필요는 없다. (그림 3)은 보안 프로그램에 대한 보안 구조의 적용을 보여준다.

보안 구조는 (그림 3)에서처럼 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 4)는 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 4) 표 형태의 보안 구조



(그림 3) 보안 프로그램에 대한 보안 구조의 적용

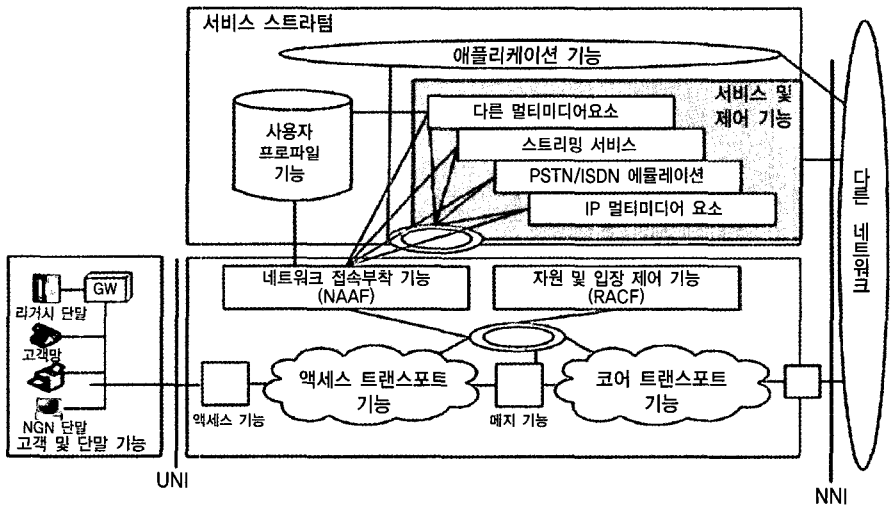
V. NGN 보안

국내에서는 아직 BcN 보안에 대한 표준이 없기 때문에, BcN의 국제적인 근간이 되는 NGN 보안과 관련하여 본 절에서 기술하고자 한다. 기본적으로 BcN은 국제적으로 정의된 차세대 네트워크(Next Generation Network : NGN) 기술인 패킷 기반의 통합 기술을 기반으로 한다. 본 장에서는 2005년 11월에 발표된 NGN 보안 릴리스 1 문서를 기준으로 NGN 보안에 대하여 기술한다[24,25].

1. 보안 구조

NGN 구조에서 네트워크는 (그림 5)처럼 응용계층과 서비스계층으로 이루어진 서비스 스트라텀(Service Stratum)과 패킷계층과 링크계층으로 이루어진 트랜스포트 스트라텀으로 구분된다. 응용계층은 서비스 제공자의 고객에 의하여 접근되는 네트워크-기반 응용을 다루며, 웹 브라우징, 전자메일 및 파일 전송 응용 등이 있다. 응용 계층의 보안은 고객과 네트워크를 보호하기 위함이다. 서비스 계층은 서비스 제공자가 고객들에게 제공하는 여러 가지 서비스들을 다루며, 도메인 이름 서비스, 부가가치 서비스, QoS 등의 서비스를 포함한다. 서비스 계층 보안은 서비스 제공자와 고객을 보호하기 위함이다. 패킷 계층은 정보 전송을 위한 패킷 플로를 다룬다. NGN에서 IP는 리거시 서비스 지원뿐만 아니라 최종 사용자에게 NGN 서비스를 제공하기 위하여 사용되는 주 프로토콜로 간주된다. 따라서 패킷 계층 보안은 IP 패킷을 보호하는데 초점을 맞춘다. 링크 계층은 직접 연결된 네트워크 설비간의 프레임 데이터 전송을 다루기 때문에, 링크계층 보안은 링크 프레임을 보호하기 위함이다.

보안을 제공하는 이런 계층 시스템은 여러 수준의 보호에 대한 고려를 하도록 한다. 예를 들어, 링크 계층은 링크 상으로 지나가는 모든 것에 대한 보호를 제공하기 때문에 거친 수준의 보안으로 생각할 수 있고, 반면에 응용 계층의 보안은 단지 해당 응용만을 보호



(그림 5) NGN 전송 및 서비스 구성

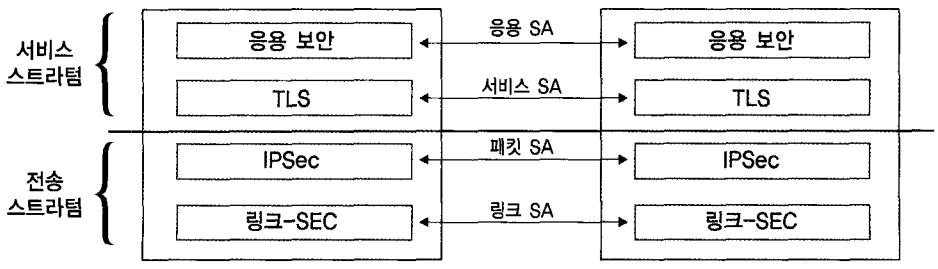
하기 때문에 미세한 수준의 보안으로 생각할 수 있다. 적절한 계층에서 동작하고 필요한 보안을 제공하는 보안 메커니즘의 선택을 위하여 비용-효율적인 해결책이 요구된다. 이에 대한 평가를 위하여 사용 패턴의 예측, 구현 계층 및 설치에 대한 고려를 하여야 한다.

2. 보안 연관

NGN에서 여러 네트워크 및 보안 계층, 보안 평면 및 스트라텀에 속하는 개체들 사이에 보안 연관(SA: Security Association)이 확립되어야 한다. (그림 6)은 NGN 보안 연관 모델을 보여준다. 보안 연관은 두 개체 사이에 안전한 전송을 위하여 인증, 암호 및 암호키 교환 방법의 협상을 정의한다. 최하위 단은 전송 스트라텀의 링크 계층을 위한 보안 연관이고, 그 상위 단에 IPSec으로 구성되는 패킷 계층을 위한 보안 연관이 존재한다. 서비스 스트라텀의 하단에 TLS (Transport Layer Security) 기능이 존재하고, 최상단에 응용 계층을 위한 보안 연관이 존재한다.

보안 연관 모델은 최종 사용자, 제어 및 관리 평면과 같이 다시 세 가지로 나누어진다. 각 평면의 보안은 개별 네트워크 활동을 보호하며, 각 평면의 보안 사이에 의존성이 없어야 한다. 즉 네트워크 제어 평면이 침해되더라도 관리 평면의 능력이 공격의 완화를 위하여 존재하여야 한다. 최종 사용자 보안 평면은 서비스 제공자의 네트워크 사용과 액세스에 대한 보안을 다루며, 또한 실제 최종 사용자 데이터 흐름을 나타낸다. 제어 평면 보안은 네트워크 사이의 정보, 서비스 및 응용의 효율적인 전달을 가능하게 하는 활동을 보호한다. 주로 머신 대 머신 통신을 포함하며, 제어 혹은 신호 정보의 보호를 수행한다. 관리 평면의 보안은 네트워크 요소, 전송 설비 등의 운영, 관리, 유지 보수 및 설비제공 기능들의 보호에 관련된다.

이외에도 3GPP/3GPP2에서는 멀티미디어 서비스 제공을 위한 IMS(IP multimedia subsystem) 구조와 보안 구조를 표준화하고 있는데, BcN에서 추구하는 음성 · 데이터 통합, 유 · 무선 통합, 통신 · 방송 융합 목표가 3GPP와 ITU에서 제시하는 IMS 표준 모델 구조의 목표와 일치한다. 그러므로 IMS 보안 구조가 BcN에서도 수용될 수 있다[2]. IMS는 SIP (Session Initiation Protocol) 프로토콜을 이용하여 All IP망에서 오디오, 비디오, 멀티미디어 컨퍼런스와 같은 IP 멀티미디어 서비스를 제공하기 위해 세션 제어방식을 정의한 차세대 통신망 구조이다. 그리고 NGN에서의 서비스와 응용을 위한 개방 플랫폼을 위한 보안 프레임워크, 비상 통신망 서비스(ETS: Emergency Telecommunications Service)와 재난복구를 위한 통신망(TDR: Telecommunication for Disaster Relief), NAT/방화벽 통과에 대한 보안 요구사항이 정의되고 있다.



(그림 6) NGN 보안 연관 모델

VI. 통합망 정보보호 추진 동향

1. BcN 보안 관련 사항

국내에서는 2005년 6월에 BcN 표준전략협의회가 구성되어 이를 중심으로 BcN 관련 국내 표준이 마련되었으며, 협의회 산하 실무분과로써 보안 분야가 구성되어 있다[7,9]. BcN 표준모델(v2.0)에서는 BcN 목표 수준에서 보안 관련 사항으로 전달망 망제어에서 통합 보안 플랫폼 구축, 가입자망 보안을 위하여 개별망 피해 확산 방지, 공격자 역추적 및 증거 수집 체계 구축을 제시하고 있다. 보다 세부적으로 전달망 계층에서 보안 및 인증 기능 제공을 위하여 다음과 같은 요구사항을 기술하고 있다.

- 보안을 위한 능동적 침해대응 체계 구축과 유해 트래픽의 침입 차단
- 망 통합 및 연동에 따른 보안피해의 확산 방지
- 이종망간의 상호연동에 따른 접근통제 및 인증
- SEN(Service Edge Node)에서 인증된 가입자 정보의 전달망 통지 및 이에 따른 자원 예약 및 트래픽 제어 기능
- 요금 및 정산을 위한 해당 정보의 기록 및 통지 기능
- 이동체의 서비스 연속성 보장을 위한 인증/권한 기술

가입자망의 요구사항으로는 유선 가입자망, 무선 가입자망, 방송 가입자망으로 구분하여 기술하고 있다. 먼저 유선 가입자망의 보안과 과금을 위하여 가입자 인증을 통한 서비스 구분 및 과금을 위하여 서비스 제어 계층 및 네트워크 제어 계층과의 연계가 필요하며, 과금을 위한 트래픽 측정 기능을 제공하도록 요구하고 있다. 또한 가입자 인증/정보(User Profile)를 활용한 유해 트래픽 원천 차단형 보안 기능을 제공할 수 있도록 기술하고 있다.

무선 가입자망의 사용자 인증 및 보안을 위하여 적법한 서비스 사용자/장치 이외 제3자의 불법적인 사용과 불법적인 액세스 네트워크의 서비스 제공을 금지하기 위한 인증 서비스와 사용자의 송수신 정보가 통신 당사자 이외의 제 3자에게 노출되는 것을 예방할 수 있는 보안 서비스 제공을 명시하고 있다.

방송 가입자망의 보안 및 인증, 권한 기능 요구사항으로 다음과 같이 기술하고 있다.

- 일반 사용자의 통신 방송 서비스 선택에 있어 인증 절차가 용이하여야 하며, 각 개별 서비스별 또는 번들로의 인증 선택이 가능하여야 한다.
- 콘텐츠의 불법 복제, 해킹으로부터의 보호에 대한 규제가 정립되어야 한다.
- 특정 서비스의 가입과 탈퇴가 용이하여야 하며, 서비스의 처리 내용의 상태를 소비자가 용이하게 알 수 있어야 한다.

홈 및 단말 계층에서 먼저 홈 네트워크의 보안 기능으로 홈 네트워크에 접속되어 있는 장치들을 보호하고 개인 사생활을 보장하는 측면에서 인증과 연동한 보안 기능을 요구하고 있다. 인증 기능으로는 홈 게이트웨이에서 외부망과 내부망 연결 시 적합한 사용자의 판별 유무와 더불어 서비스 유형에 따른 사용자에 대한 인증 기능 수행을 기술하고 있다.

[9]에서 제시하고 있는 네트워크 보안의 주요 목표를 정리하면 <표 2>와 같다.

〈표 2〉 네트워크 보안의 단계별 주요 목표

단계	주 요 목 표
1단계	- DDoS 및 Worm 등의 해킹 공격에 대응능력을 갖는 보안시스템 확보 - 국가적인 차원의 통합보안체계 마련 및 주요 사업자의 통합관제센터 구축
2단계	- 서비스/제어망, 전달망 및 가입자망에서 유해 트래픽 실시간 감시 및 차단 시스템 구축 - 사업자별 네트워크 통합형 보안관리 시스템 구축 및 망연동을 위한 상호 인증체계 마련
3단계	- 능동적으로 위험 요소를 찾아 차단 및 추적할 수 있는 보안시스템 구축 - 통신, 방송, 신규서비스(USN, RFID), 홈네트워크 등)에 대한 통합보안 관리 시스템 및 통합인증 체계 구축

주요 고려 사항은 다음과 같다.

- Circuit 개념이 적용된 BcN 전달망에서 네트워크 보안 방안
- BcN 인프라 대비 네트워크 보안장비의 성능저하에 따른 보안취약점 문제
- 망 통합 및 연동에 따른 보안피해의 확산 방지 고려
- 유무선, 방송환경에서의 도감청 및 데이터 위·변조 방지
- 이종망간의 상호연동에 따른 접근통제 및 인증 관련 취약성 고려
- IPv4와 IPv6의 병행사용에서의 End-to-End 보안 확보 방안

BcN 보안을 위한 추진 방향은 다음과 같이 기술하고 있다.

- ㅇ 정책적으로 보안에 대한 준수 기준 마련
  - 사업자의 보안관리체계 수립 및 통합보안관리센터 구축 의무화
  - 네트워크 보안장비의 필수기능에 대한 인증제
  - 사업자 및 Service Provider에 대한 보안평가 등급제 실시
- ㅇ보안 표준 추진
  - 장비의 상호호환성 확보를 위하여 규격 및 보안기술의 인터페이스 표준 추진
  - BcN의 통합서비스 제공이 가능할 수 있도록 통합인증 표준 마련

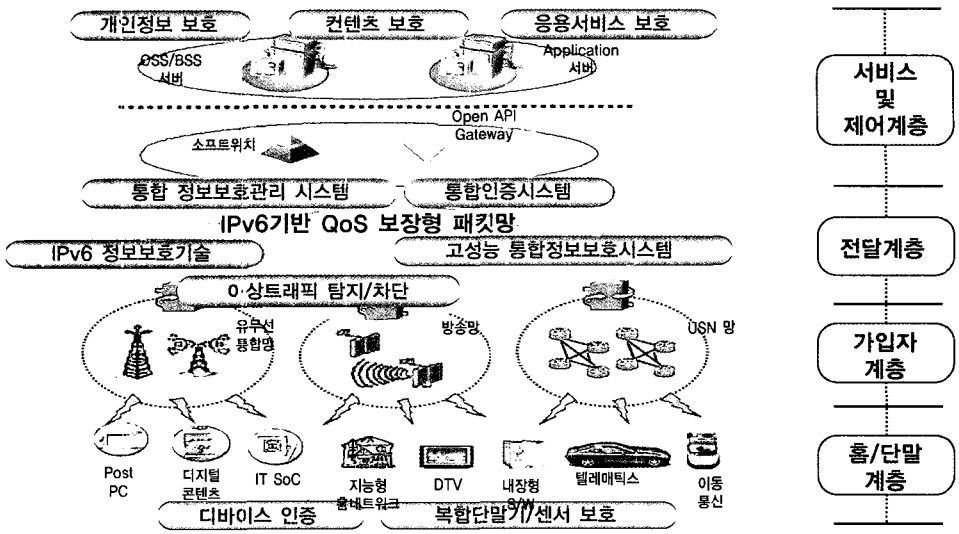
2. 통신망 정보보호 기술개발 내용

BcN 통합환경에서 체계적으로 침해사고에 대처하기 위하여 통합정보보호 관리체계를 구축하고자 계획을 수립하고 있다[7]. 본 계획에서는 정보보호 기술의 고도화 및 정보보호체계 통합화를 통하여 안전하고 신뢰성 있는 건전한 사이버 네트워크 환경 구축을 목표로 한다. 본 절에서는 주요 내용에 대하여 살펴본다. (그림 7)은 BcN 보안망 체계도를 보여준다.

BcN 정보보호 기술 개발 내용은 다음과 같다.

- ㅇ고성능 통합 네트워크 정보보호 기술 개발
  - 보안 장비간 연동을 통해 전체 망을 보호하는 동시에, 서비스 품질에 영향을 최소화하는 QoS-aware 통합 정보보호 기술 개발
  - 다양한 응용서비스를 통한 공격에 대응하기 위해 컨텐츠 기반의 DoI(Denial of Information) 공격방지 기술 개발
- ㅇ 사용자의 네트워크 접속인증 및 서비스 인증과, 이기종망간 핸드오프 시 마다 수행되는 인증절차를 통합하는 통합인증기술 개발
- ㅇ 사용자 인증을 위한 생채인증 기술 고도화 및 사용자 생채정보보호 기술 개발
- ㅇ 금전적인 피해 등을 유발하는 침해사고의 증가로 인한 사이버 범죄 수사를 위한 공격자 위치 추적 및 컴퓨터 포렌식(Forensics) 기술 개발
- ㅇ 단말 및 응용 서비스를 보호하기 위한 정보보호 기술개발
  - VoIP 서비스의 음성 데이터 보호를 위한 실시간 고속 암호화 기술 및 VoIP 스팸 대응 기술 개발
  - 안전하고 편리한 홈서비스 제공을 위한 디바이스 인증 및 능동보안 인지기술 개발
  - 낮은 성능, 저용량의 소형 단말기를 고려한 경량 침해방지 기술 및 개인정보 유출 방지 기술개발
- ㅇ 다양한 서비스를 통해 제공되는 방송, 멀티미디어 등의 컨텐츠에 대한 지적재산권 보호 기술

추진일정은 3단계로 구분되어 이루어지며, 이미 1단계 사업(2004~2005년)은 완료되었다. 2단계 사



(그림 7) BcN 보안망 체계도

업은 올해부터 2년간, 마지막 3단계 사업은 2008년부터 2010년까지로 계획되어 있다. 3단계 사업이 완료되는 시점에는 위에서 제시된 모든 기술들이 개발될 것으로 예측된다. 보다 자세한 내용을 위하여 [7,9]를 참조할 수 있다.

VII. 맺음말

통합망 서비스의 수용이 가능한 네트워크 모델을 수립하고 BcN 구축 및 서비스 분야의 표준화를 실현하기 위하여 망 구조, 기술 및 서비스 제공기준에 대한 지침으로 BcN 표준모델이 개발되었다. 이에 따라 BcN 보안 분야에서도 표준화가 추진되고 있다.

본 논문에서는 BcN 보안의 필요성과 기술, 국내 BcN 보안 표준 확립을 위하여 참고가 될 수 있는 ITU-T X.805 종단간 네트워크 보안 표준과 NGN 보안 구조에 대하여 기술하였다. 그리고 국내에서 추진되고 있는 통합망 정보보호 추진동향에 대하여 알아보았다.

국가적으로 추진하고 있는 유비쿼터스 사회를 앞당기기 위하여 정보보호 문제는 간과될 수 없는 중요한 이슈로 생각된다. 이를 위하여 산 · 학 · 연 · 관이 상호 협력 및 역할 분담을 통하여 정보보호 표준화가 성공적으로 추진되어야 하며, 아울러 관련 정보보호 기술 개발이 이루어져야 한다.

[참 고 문 헌]

[1] 김국한, 최병철, 유종호, 서동일, "BcN 정보보호 기술개발 현황", 인터넷정보학회지, 제6권 제3호, pp.72-82, 한국인터넷정보학회, 2005년 9월.

[2] 박재구, 남일성, "IMS 기술동향 및 BcN에서의 적용구조", 인터넷정보학회지 제6권 제3호, pp.32-41, 한국인터넷정보학회, 2005년 9월.

[3] 서동일, "IT839 정보보호 표준화 현황과 전망", 한국통신학회지 제22권 제8호, pp.1003-1014, 한국통신학회, 2005년 8월.

[4] 신승원, 오진태, 김기영, 장종수, "인터넷 웜 공격 탐지 방법 동향", 전자통신동향분석, 제 20권 제1호, pp.9-16, 2005년 2월.

[5] 염흥렬, "종단간 네트워크 보안 표준과 NGN 보안 구조", 정보통신기술, 제19권 제2호, pp.2-14, 한국정보과학회 정보통신연구회, 2005년 12월.

[6] 전용희, 장종수, "BcN 인프라 정보보호", 정보보호학회지 제15권 제3호, pp.13-28, 한국정보보호학회, 2005년 6월.

[7] 정보통신부 BcN 구축 연동 계획(2. 통합망 정보보호 체계 고도화), 작업문서, 2005년 12월, BcN보안 소분과.

[8] 최양서, 장종수, "BcN 인프라 정보보호", 한국통신학회지 제22권 제8호, pp.1015-1024, 한국통신학회, 2005년 8월.

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

[10] Cliff C. Zou et al., "Monitoring and Early Warning for Imternet Worms", Proc. of 10th ACM Conf. Computer and Comm. Security(CCS 03), pp.190-199, Oct. 2003.

[11] Cynthia Wong, Chenxi Wang, Dawn Song, Stanley M. Bielski, and Gregory R. Ganger, "Dynamic Quarantine of Internet Worms", The International Conf. on Dependable Systems and Networks (DSN-2004), pp.62-71, 2004.

[12] Cynthia Wong, Stan Bielski, Ahren Studer, Chenxi Wang, On the Effectiveness of Rate Limiting Mechanisms, CMU-PDL-05-103, Carnegie Mellon University, March 2005.

[13] Gregory R. Ganger, Gregg Economou, and Stanley M. Bielski, Self-Securing Network Interfaces: What, Why and How. Technical Report.

[14] Helen J. Wang et al., " Shield: Vulnerability-Driven Network Filters for Preventing Known Vulnerability Exploits", Proc. of ACM SIGCOMM '04, Aug. 30-Sep. 03, 2004, USA.

[15] Hyang-Ah Kim and Brad Karp, " Autograph: Toward Automated Distributed Worm Signature Detection", Proc. of Usenix Security Sym., pp.271-286, 2004.

[16] ITU-T Rec. X.800(1991), Security Architecture for Open Systems Interconnection for CCITT Applications.

[17] ITU-T Rec. X.805(2003), Security Architecture for Systems Providing End-to-end Communications.

[18] Matthew M. Williamson, "Throttling Viruses: Restricting propagation to defeat malicious code", Proc. of ACSAC Security Conference, pp.61-68, 2002.

[19] Min Cai et al., "Collaborative Internet Worm Containment", IEEE Security and Privacy, pp.24-33, May/June 2005.

[20] N. Weaver, S. Staniford, and V. Paxon, "Very Fast Containment of Scanning Worms", Proc. of 13th USENIX Security Symposium, pp.29-44, August 2004,

California.

[21] Shigang Chen and Yong Tang, "Slowing Down Internet Worms", Proc. of 24th IEEE International Conference on Distributed Computing Systems (ICDCS' 04), Tokyo, Japan, March 2004.

[22] Stelios Sidiroglou and Angelos D. Keromytis, "Countering Network Worms Through Automatic Patch Generation", IEEE Security and Privacy, 2005.

[23] Stuart E. Schechter, Jaeyoun Jung, and Arthur W. Berger, "Fast Detection of Scanning Worm Infections", Proc. of 7th International Symposium on Recent Advances in Intrusion Detection (RAID), Sep. 2004, France.

[24] Takashi Egawa, Security Requirements for NGN Release 1, ITU-T FGNGN-OD-00255, Nov. 2005.

[25] Zachary Zeltsan, Guidelines for NGN Securiy Release 1, ITU-T FGNGN-OD-00254, Nov. 2005.

전용희

1971년 ~ 1978년 고려대학교 전기공학과
1985년 ~ 1987년 미국 플로리다공대 대학원 컴퓨터공학과
1987년 ~ 1992년 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 ~ 1978년 삼성중공업(주)
1978년 ~ 1985년 한국전력기술(주)
1979년 ~ 1980년 벨기에 벨가톰(Belgatom)사 연수
1989년 ~ 1989년 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 ~ 1992년 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA
1992년 ~ 1994년 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 ~ 현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년 ~ 2003년 동 공과대학장 역임
2004년 ~ 2005년 한국전자통신연구원 정보보호연구단 초빙연구원
2005년 ~ 현재 BcN Forum 보안 소분과 위원, BcN 보안 표준 분과위원
관심분야 : BcN 보안 및 QoS 보장 기술, 네트워크 보안, 통신망 성능 분석