BcN 정보보호 위협과 발전방향

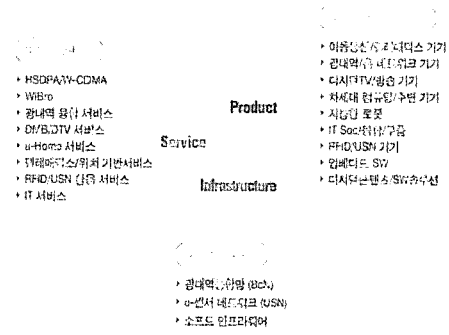
특집 07

목 차

임채태 · 원유재
(한국정보보호진흥원)

1. 서 론

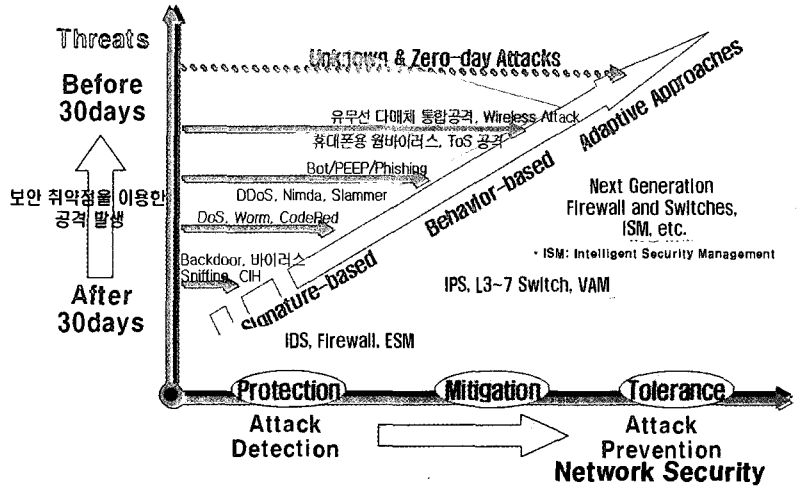
우리 경제의 주요 기반인 IT 산업을 경쟁력 높은 미래형으로 끌어올리기 위해 u-IT839 전략을 수립하여 추진하고 있다. u-IT839 전략은 (그림 1)에서 보여주듯이 8개 핵심서비스와 3대 핵심인프라 그리고 9대 신성장동력을 정의하고, 각각에 대한 보급시기, 기술개발 방법 및 목표 등을 포함한 중·장기 계획을 수립하여 추진 중에 있다.



(그림 1) u-IT839 전략

3대 인프라에서 BcN은 이기종망의 통합 및 연동이 이루어지는 기본 인프라로써, 새로운 신규 서비스가 BcN 기반위에서 개발되고 있다. BcN이 발전하면 유·무선, 음성·데이터, 방송·통신망이 통합되어 정부, 기업, 개인에게 다양한 서비스를 제공할 수 있을 것이다.

BcN 구축을 위해, 정부에서는 2010년까지 총 3단계로 시범사업을 추진하고 있으며, 1단계 시범사업이 2005년을 기점으로 종료되고, 2006년부터 2007년까지의 2단계로 접어들었다. 1단계 시범사업을 통해 광대역, 유·무선 통합, 음성·데이터 통합 등이 이루어 졌으며, 품질보장을 위한 기반기술이 구축되어 전국 12개 지역 2076가구에 광대역, 품질보장형 서비스를 제공하였으며, 2단계에 접어들면서 품질보장 기술고도화 및 타 사업자 망간의 연동 고도화를 지속적으로 추진하고, 신규 응용서비스를 중점적으로 발굴하여 BcN 서비스의 대중화를 가속화하는 목표를 가지고 적극 추진하고 있다. 또한, 금년부터는 이제까지 추진된 인프라와 서비스 분야의 노력을 통



(그림 2) 사이버 공격의 고도화 추세

합하여 시너지를 높일 수 있도록 u-City 및 u-Work 사업을 추진하여 입체적으로 유비쿼터스 사회로의 진입을 가속화 시킬 계획이다.

초고속 정보기반의 확산과 더불어 인터넷뱅킹의 해킹사고, 다양한 변종의 웜·바이러스 등장, 휴대폰용 웜·바이러스 출현 등에서 볼 수 있듯이, 정보사회의 발전과 병행하여 다양한 정보화 역기능이 증가하고 있는 것이 현실이다. 2005년까지 순기능 중심으로 u-IT839 전략이 추진되었다면, 이제부터는 3대 인프라 및 여러 신규서비스의 상용화에 발맞추어 보안을 함께 고려하여 안전한 서비스를 제공하는 것이 중요하며, 이를 통해 사용자 신뢰를 확보하고 서비스가 보다 원활하게 보급될 수 있는 선순환 구조를 만들어 나가야 할 것이다.

따라서, 본 고에서는 유비쿼터스 사회로 가기 위한 초고속 정보기반 환경의 변화를 살펴보고 예상되는 정보보호 위협요소를 도출한 후, 정보보호 위협에 대비한 정보보호 추진방향을 제언하고자 한다.

2. 정보보호 환경의 변화

최근 들어 사이버공격은 이전의 시스템 침입이나 웜·바이러스로 인한 파일 변조, 자료 유출 등 개별시스템과 개인에 대한 공격에서 원격 조정이 가능한 해킹도구의 사용을 통한 특정 목표 공격이나, 웜·바이러스 등을 통해 대량의 트래픽을 발생시킴으로써 인터넷 망 기반구조를 공격하는 형태로 변화되고 있다. 더욱 심각한 것은 최근의 사이버 공격이 금전적인 이익을 목적으로 하는 사이버 범죄가 크게 증가하고 있다는 점이다. (그림 2)는 사이버 공격의 고도화 추세를 보여주고 있으며, 이에 대응하기 위한 보안기술 개발 동향을 보여주고 있다.

2.1 사이버 공격의 지능화, 고도화, 고속화

최근의 사이버공격은 웜·바이러스에 취약점 자동스캔, 자체 메일발송엔진, 감염 PC 원격제어 등 해킹 기술이 결합되어 능동적으로 확산대상을 탐색하고, 감염시킨 대상을 특정 사이트를 공격하는 중간경유지로 악용하는 등 고도화되고 있다. 또한 이러한 해킹 프로그램 및 웜·바이러스 소스가 인터넷에 공개되고, 공개된 해킹 프로그램 및 웜·바이러스 소스프로그램을 통해 전문지식이 없는 일반인도 쉽게 해킹 기술을 익히고, 누구라도 사이버공격을 감행할 수 있게 되었

다. 이러한 경향에 따라 최근의 웜·바이러스는 다양한 악성 변종들이 급속하게 확산되고 있고, 광범위하게 확산된 변종들에 의하여 백신 등 방어체계가 무력화되는 등 부작용이 심각해지고 있다. 또한, 소프트웨어에 보안취약성에 대한 공격 추이를 보면, 보안취약성의 발표 후 이에 대한 공격이 이루어지는 기간이 점점 짧아지고 있으며 최근에는 취약점에 대한 패치가 발표되기 전에 공격이 이루어지는 Zero-Day 공격으로 발전하여 그 위협이 크게 증가하고 있다.

2.2 전파경로의 다양화

과거의 공격전파 유형은 PC통신 등을 통한 파일 다운로드나 디스켓의 복제 등 사용자의 행위가 반드시 개입되어야 했었다. 하지만, 최근의 확산 방식은 이전과 달리 소프트웨어에 내재된 취약점을 악용하거나, 이메일에 웜 자체를 첨부하여 전송함으로써 불특정 다수에게 전파시키거나, 공유 폴더, P2P 등과 같이 최근 보편화된 네트워크 서비스를 통하여 감염을 시도하는 등 전파경로가 다원화되어 가고 있다.

특히, 메일로 전파되는 웜들은 메일서버를 경유하여 전파하는 것보다 신속하게 자신을 복제하기 위하여 메일전송 프로그램을 내장하고 있으며, 메일의 제목이나 본문의 내용을 수신자가 읽어보도록 현혹시키는 사회공학적 수법을 가미하는 등 전파 수법이 매우 지능화되고 있어 이로 인한 피해가 급속히 늘어나고 있다.

2.3 사회공학적 역기능의 증가

기존의 과시형 공격 또는 특정 대상에 대한 공격에서 점차로 인터넷 뱅킹 사고 등과 같이 범죄의 수단으로 사용되는 경우가 지속적인 증가 추세를 보이고 있어 그 심각성은 날로 심화되고 있다. 또한, 경제·사회활동 등 생활전반에 걸쳐 인터넷 의존도가 점차로 심화됨에 따라 많은 개인정보가 인터넷에 저장되고 있으며, 그로인해 사용자의 프라이버시 침해에 대한 우려가 급속히 증가하고 있는 추세이다.

마지막으로, 불특정 다수에 대한 무작위적인 스팸 메일 또는 메시지가 증가함에 따라 인터넷 사용자에게 불편함과 거부감을 유발시키고 있으며, 각 개인의 피해를 떠나 점차 사회문제화 되고 있다. 하지만, 점차로 스팸이 단순 광고 수준에서 벗어나, 사회공학적 수법을 통한 개인정보의 불법적 취득, 악성코드 삽입을 통한 공격 경유지화 등, 제 2의 사이버 공격 혹은 범죄의 수단으로 사용되고 있다는데 더 큰 문제가 있겠다.

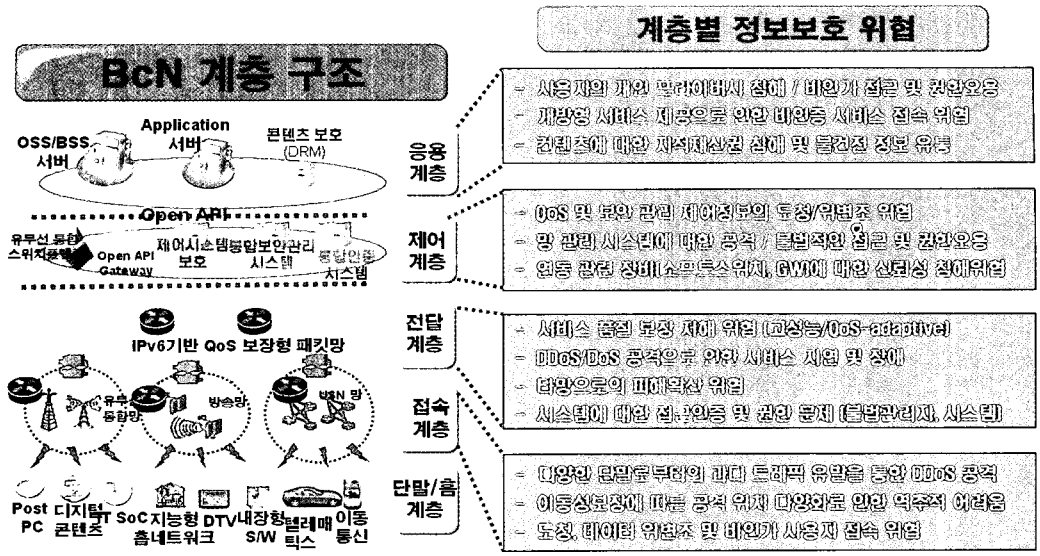
3. BcN 정보보호 위협

광대역 통합 환경인 BcN에서는 기존 인터넷 망에 잠재된 취약점과 더불어 신규 구성요소 및 기술의 적용으로 인한 새로운 보안위협이 나타날 것으로 예측된다. 첫째, 네트워크의 광대역화로 악성코드의 전파 역시 급속하게 진행되어 취약한 네트워크 기반을 빠른 속도로 마비시킬 수 있다. 둘째, 기존에 별도로 운영되고 있는 음성·데이터, 유·무선, 통신·방송이 통합되어 구성·운영되므로 공격에서 상대적으로 안전했던 전화망, 방송망으로 피해범위확산이 우려된다. 셋째, 휴대폰, PDA, RFID 내장, WiBro, DMB 등 기능이 융합된 복합 단말기를 대상으로 한 해킹 및 웜·바이러스가 발생할 것으로 예측되며, 이는 현재의 개인용 PC에 의한 공격보다 더욱 위협적일 것으로 예측된다.

BcN을 그 기능에 따라 계층별로 구분하면 (그림 3)에서와 같이 서비스 및 제어계층, 전달계층, 접속 계층, 단말 및 홈네트워크 계층으로 구분되며 네트워크 인프라가 아닌 단말 및 홈네트워크 계층을 제외한 각 계층별 정보보호 위협들을 살펴보면 다음과 같다.

3.1 서비스 및 제어 계층의 정보보호 위협

서비스 계층은 Open API를 기반으로 다양한



(그림 3) BcN 계층별 정보보호 위협

인터넷 접속기술을 사용하는 사용자에게 쉽게 다양한 서비스를 제공할 수 있는 구조를 가진다. 이러한 개방형 구조를 가짐으로써, 비인가 서비스의 접속으로 인한 불법 서비스 제공 위협, 다양한 멀티미디어 콘텐츠에 대한 지적재산권 침해 위협 및 불건전 정보의 유통위협들이 존재한다. 또한, 기존인터넷에서와 마찬가지로 응용서비스에 대한 비인가 사용자 접근 및 권한오용 위협과 서비스 사용자의 개인정보에 대한 프라이버시 침해 위협들이 존재한다.

제어계층은 이기종망간 연동, 네트워크 자원, 망장비, 인증, QoS 등을 제어·관리하는 역할을 담당하는 BcN의 핵심 계층으로써 여러 종류의 제어 및 관리정보에 대한 불법적인 도청과 위변조 위협이 존재한다. 또한 유·무선 및 음성·데이터 통합을 위한 교환시스템, 사용자 및 관리자가 합당한지 검증하기 위한 인증서버, 네트워크 자원을 관리하기 위한 자원관리서버 등과 같은 중요 제어 시스템에 대한 공격으로 인한 피해는 2003년 발생한 1.25 인터넷 침해사고와 같이 네트워크 전체에 영향을 미칠 수 있으나, 인터넷의 존도가 점차 심해지는 현 상황에서, 그 피해는 더욱 클 것으로 예상된다. 앞서 살펴본 서비스 및 제어계층에 대한 정보보호 위협을 정리하면, 다음 <표 1>과 같다.

<표 1> 서비스 및 제어계층의 정보보호 위협

보안 위협	내용
사용자의 개인정보 및 관리 제어 정보의 유출 및 위변조	- 사용자의 개인 정보(ID, 주민번호 등)의 불법적인 유출 및 위변조 - 관리제어 정보들이 노출 및 위변조
서비스에 대한 불법 접근 및 권한 오용	- 응용 서비스에 대하여 불법적인 사용자가 접근 - 본래 부여된 권한을 초과하여 서비스 이용
개방형 API 제공으로 인한 비인증 서비스의 접속	- 비인증 응용서버들이 쉽게 접속 - 불법적인 서비스 제공 및 서비스 가로채기
지적 재산권에 대한 침해	- 응용서비스 컨텐츠에 대한 지적재산권 침해
새로운 Protocol의 사용에 대한 취약성 악용	- 검증되지 않은 프로토콜 자체의 보안 취약성 악용한 공격
사용자 세션 하이젝킹 위협	- 불법적으로 사용자의 세션을 가로채거나, 해제할 수 있음
소프트스위치(IMS) 및 게이트웨이의 비정상 동작	- 악의적인 공격으로 비정상적으로 동작할 수 있음 - 핵심역할을 담당하는 구성요소로 장애 시, 서비스 제공 불능

3.2 전달 계층의 정보보호 위협

전달계층은 광통신 기술을 이용하여 높은 대역폭을 제공하고 MPLS 기술이 적용된 라우터를 통해 서비스 품질을 보장한다는 점이 가장 큰 특징으로써, 특정 서비스 품질을 저해하거나 악의적인 제어 메시지 전송을 통한 임의의 대역폭 할당 및 타인의 대역폭 축소 등의 공격위협이 존재한다. 또한, 광대역 환경에서 악의적인 대량트래픽 발생을 통한 DDoS 공격위협은 기존의 환경에서와 같이 상존하나, 그 피해는 인터넷 망에 국한된 피해가 아니라, 다양한 이기종망까지 그 피해가 확산되는 광범위한 피해를 유발할 것으로 예상된다. 전달계층에 대한 정보보호위협을 정리하면 아래 <표 2>와 같다.

〈표 2〉 전달계층의 정보보호 위협

보안 위협	내용
전달망 측면에서의 서비스 품질 저해 및 불법 할당 위협	- 대역폭을 불법적으로 사용 - 특정 대상의 할당 대역폭을 사용하지 못하게 하는 공격
이종망간 상호 연동 방해 및 불법트래픽 유입	- 연동을 방해하는 공격이 발생 - 연동과정에서 사용자 정보 노출 - 인가되지 않은 불법 트래픽의 유입
DoS 공격으로 인한 서비스 지연 및 장애	- DoS 및 DDoS 공격을 통한 인터넷의 마비 - 악의적인 공격 혹은 기타 원인으로 인터넷 기반 서비스 중단
IPv4와 IPv6의 혼합 사용으로 인한 취약성 악용 공격	- IPv4와 IPv6 연동 취약점 악용 - 보안정책이나, 여러 보안기능의 적용 측면에서 어려움

3.3 접속 계층의 정보보호 위협

접속계층은 유선망, 무선망, 방송망으로 구분되며 광대역과 이동성을 보장하기 위한 접속기술이 점차 확대되고 있다. 접속계층에서는 다양한 단말로부터의 과다 트래픽이 네트워크로 유입될 수 있으며, 이동성 보장에 따른 공격자 위치의 다양화로 역추적이 어려울 수 있다. 또한, 기존과 마찬가지로 사용자 데이터에 대한 도청위협이 상존하며, 특히 전송매체를 공유하는 무선망에서 보다 취약할 것이다. 접속계층에 대한 정보보호위협을 정리하면 아래 <표 3>과 같다.

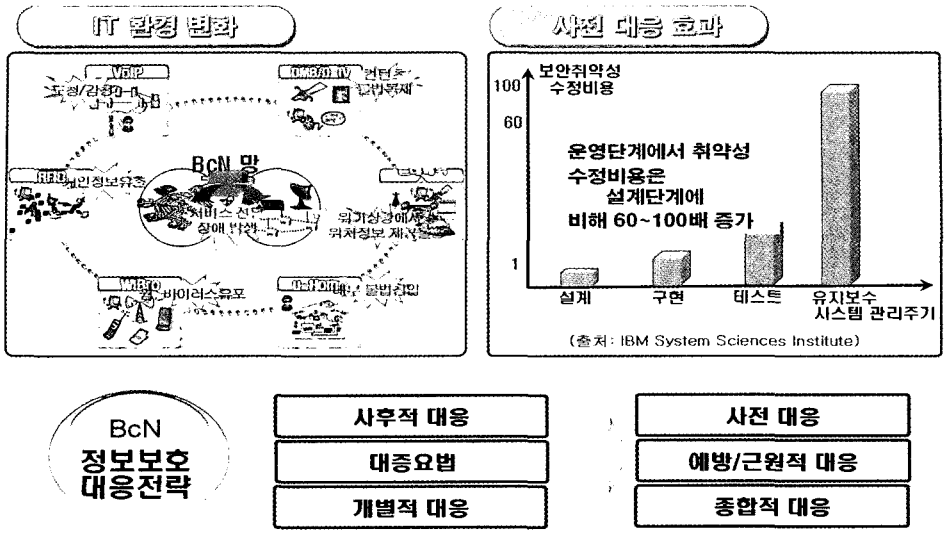
〈표 3〉 접속계층의 정보보호 위협

보안 위협	내용
망 통합으로 인한 취약성 확산	- 개별망의 취약성으로 인한 피해는 모든 망으로 확산될 수 있음
악의적 공격의 위치 다양화 및 역추적 어려움	- 이동성이 보장되는 환경으로써, 악의적인 공격자의 위치는 매우 다양하여 역추적에 있어서도 어려움
비인가 사용자의 불법 접속	- 다양한 접속망을 동시에 이용할 수 있는 환경 (복합단말기)
DHCP 주소 공간 고갈 공격	- 정상적인 사용자가 망에 접속하는 것을 방해
유·무선망 도청, 데이터 위변조	- 음성 데이터 및 기타 멀티미디어 서비스 피해
Jamming 공격	- 무선 및 방송망에 jamming 공격 (QoS 보장하기 어려울 수 있음)
MITM(Man in the middle) 공격	- 다양한 무선 망 (WLAN, WiBro 등)

4. BcN 정보보호 대응전략 및 대응방안

4.1 BcN 정보보호 대응전략

기존의 정보보호 대응은 보안 사고가 발생한 후, 원인을 분석하여 대응하는 사후적 조치와 각각의 서비스 및 접속망별로 개별적으로 이루어져 왔다. 하지만, 보안사고 후 대응하는데 소요되는 비용과 비교하여 설계단계에서부터 보안을 반영하여 서비스를 구축하는 것이 훨씬 경제적이라는 여러 보고에서 알 수 있듯이 서비스가 본격 상용화되기 이전 설계·구축단계부터 보안을 고려하는 사전대응이 필요하다. 또한, 점차 중요 서비스가 BcN 기반 위에서 제공되고, 인터넷 의존도가 심화됨에 따라, 정보보호 사고로 인한 피해가 상당히 클 것으로 예상되므로, 보안위협의 철저한 분석을 바탕으로 사전에 예방하는 근원적 대응이 필요하다. 마지막으로, BcN은 다양한 이기종망의 통합 환경으로써, 기존의 개별적 보안대응은 매우 복잡하고 어렵게 만들 수 있으므



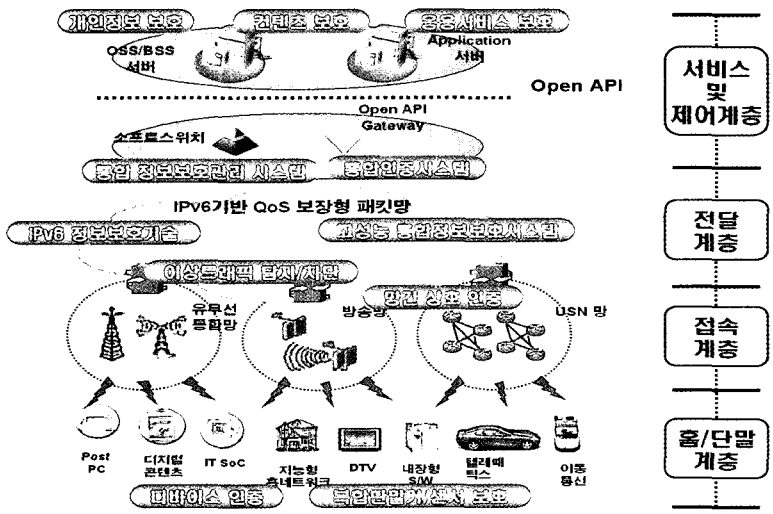
(그림 4) BcN 정보보호 대응전략

로, 종합적인 대응이 필요하다.

4.2 BcN 계층별 정보보호 대응방안

BcN 정보보호 위협에 대비하여 BcN 계층별로 적용되어야할 주요 정보보호 요소들을 (그림 5)에서 간략하게 보여주고 있으며, 각 계층별 기술적 대응방안 다음과 같다.

서비스계층에서는 응용서비스에 대한 불법접근 및 권한오용을 방지하기 위해 접근제어 및 AAA 등 강한 인증기술이 적용되어야 하며, 프라이버시 침해방지를 위해 사용자 암호화 기법 및 정보에 대한 접근제어 등 개인정보보호 기술이 적용되어야 하며, 다양한 컨텐츠에 대한 지적재산권 보호(DRM) 기술이 적용되어야할 것이다. 또한,



(그림 5) BcN 주요 정보보호 요소

Open API 기반 환경에서 제공되는 서비스가 올바른 서비스인지 검증하기 위한 서비스 인증 기술이 적용되어야 하며, 개방형 서비스구조의 기반 프레임인 OSA(Open Service Access) Gateway 시스템을 보호하기 위한 시스템 보호 기술이 적용되어야 한다.

제어계층에는 여러 계층에 산재되어 있는 개별 정보보호 장비간 연동 및 제어를 통해 전체 네트워크를 보호할 수 있는 통합정보보호관리 기술이 적용되어야 하며, 보안관리, 과금, QoS 관리 등 중요 제어 시스템의 신뢰성을 보장할 수 있는 기술이 적용되어야 한다. 또한, 제어 및 설정정보의 유출 및 위변조를 방지하기 위해 암호 및 접근제어 기술이 적용되어야 하며, 원격에서 시스템을 관리하는데 있어서 정보 유출을 방지하기 위해 SSL, IPSec 등의 보안기능이 적용되어야 할 것이다. 마지막으로, 여러 게이트웨이 및 교환시스템과 같은 코어 시스템을 보호하기 위해 Secure OS 등의 시스템 보호기능과 장애가 발생하더라도 서비스를 제공할 수 있도록 장애허용 기술이 적용되어야 한다.

전달계층에서는 백본 네트워크의 처리능력에 따른 능동 고성능 네트워크 보안기술이 필요하며 사이버 공격이 지능화, 고속화, 다양화됨에 따라 DDoS 공격에 대응할 수 있는 지능형 이상트래픽 탐지기술이 마련되어야 하며, 이에 대응하기 위해 기존의 ACL 및 rate-limit 등의 공격트래픽 제한기법과 Black hole, sink hole 등의 공격트래픽 완화기법이 BcN 환경에 적합하도록 적용되어야 한다. 또한, VoIP 서비스와 같이 민감한 서비스를 인식하여 서비스 품질에 영향을 최소화하기 위해 Best effort 트래픽과 차별을 두고 대응하여야 할 것이다. 더불어, 서비스 품질 저해 공격에 대응하기 위해 QoS 관련 제어 메시지에 대한 기밀성 및 무결성을 보장하기 위한 메시지 암호화 및 인증기술이 적용되어야 할 것이다.

접속계층을 살펴보면, 사용자로부터의 유해트래픽을 사전에 탐지하고 차단하여 전달계층에 피해가 미치는 영향을 최소화해야 하며, 이기종 망간의 연동에 있어서 불법 트래픽의 유입을 막기 위해 망간 상호인증이 필요하다. 또한, 공격자 추적을 위해 이동 단말에 대한 로그정보 등 정보를 통합보안관리 시스템에 제공하여야 하며, 상대적으로 접속계층은 도청위협에 크게 노출되어 있으므로 사용자의 메시지 송수신 시 암호화 기법이 적용되어야 한다. 더불어, 불법 사용자의 비인가 접속 및 중간자 공격을 방지하기 위하여 공개키 기반의 강력한 사용자 인증 기법이 적용되어야 할 것이다.

4.3 안전한 BcN 환경 구현을 위한 정책적 대응방안

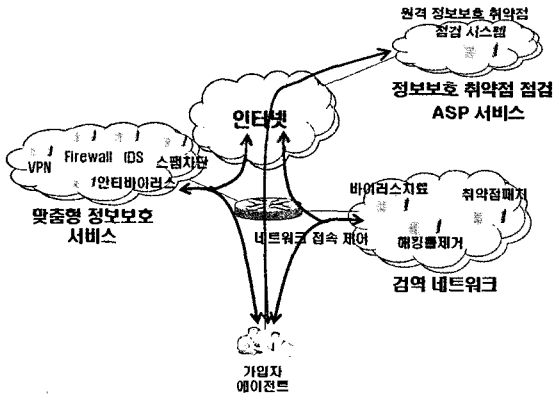
BcN 망은 이기종망간, 타사업자간 연동되는 통합망이므로 특정 취약망의 피해로 인해 대다수 사용자에게 안전한 서비스를 제공하지 못할 수 있다. 따라서 침해사고에 효과적으로 대응하기 위한 이기종망 및 타사업자와의 협조체계가 필요하다. 서로 정보보호 위협 및 침해사고 정보를 공유하고, 대응전략을 수립하는 등의 통합보안관리 체계가 구축되어야 할 것이다.

BcN은 서비스 품질을 보장하는 네트워크이다. 하지만, 다양한 접속기술을 가지는 복합단말기의 등장에 따른 접속망 변경과 단말기의 이동성에 따른 핸드오프로 인하여 빈번한 인증절차를 요구하게 되며, 이로 인해 서비스 품질저해와 사용자 불편을 유발할 수 있다. 따라서, 서비스 품질에 영향을 최소화하고 사용자의 편리성을 도모하기 위해 통합인증 기술이 마련되어야 한다.

현재, 2단계 BcN 시범사업을 추진하고 있는 시점에서, 본격적인 상용화에 앞서 정보보호 위협을 분석하고, 대응방안을 마련하여야 한다. 안전한 BcN 환경구축을 위해 BcN 시범사업에 대한 정보보호 안전성 점검을 통해 세부대책을 마련하도록 하고, 연구소 및 정보보호 업체에서는 BcN에 필요한 기술 및 제품을 개발하도록 유도

하는 노력이 필요하다.

많은 인터넷 침해사고에서 트래픽의 진원지는 감염단말기로 파악되고 있다. 이에 따라 가입자 단말기에 대한 정보보호의 필요성이 크게 중요시되고 있으며, 가입자 망에서 유해트래픽에 대한 사전 탐지 및 차단기능에 대한 요구가 증가하고 있다. 따라서 가입자 단까지 보안기능을 확대하여, 유해트래픽을 사전에 차단할 수 있는 체계 구축이 필요하다.



(그림 6) 정보보호 시범서비스

마지막으로, 정보보호는 어느 한부분에서 대비한다고 이루어지는 것이 아니라, 사업자, 정부, 기업, 개인 등 모두가 역할을 수행하여야 한다. 일반적으로, 가입자들은 정보보호 측면에서 인식이 부족하며, 중소기업은 정보보호를 위해 투자하기에 여력이 없다. 또한, 사업자 측면에서는 안전한 서비스 제공을 위해 다양한 정보보호 서비스를 기획하고 있다. 따라서, (그림 6)과 같이 인식이 낮은 가입자에 대하여 안전하게 통신할 수 있도록 하고, 중소기업에서는 저렴한 가격으로 원하는 수준의 정보보호 서비스를 제공받도록 하며, 정보보호 서비스를 준비하고 있는 사업자는 서비스에 대한 검증을 수행할 수 있도록 하는 정보보호 시범서비스를 고려할 수 있다. 결국, 정보보호 서비스가 보편화 된다면, 전체 통신환경도 보다 안전한 환경으로 정착될 것이다.

5. 결 론

3대 인프라중 하나인 BcN은 이기종망의 통합 및 연동이 이루어지는 기본 인프라로써, 2004~2010년까지의 BcN 시범사업을 통하여 멀지 않은 미래에 본격적인 상용화가 이루어질 것이며, 이를 기반으로 다양한 서비스가 광범위하게 제공되어 유비쿼터스 사회로의 진입을 가속화 시킬 것이다. 반면, 최근의 사이버공격은 시스템 및 네트워크의 취약점을 악용하여 고속으로 전파되는 양상을 띠고 있으며, 웜·바이러스 및 해킹 기술이 결합되어 공격의 확산속도와 파괴력은 점점 커지고 있다. 또한, 최근에는 위장 사이트와 이메일을 이용하여 개인 정보를 수집하는 피싱(Phishing) 기법을 사용하여 타인의 은행 예금을 불법 인출하는 사고가 증가 추세에 있으며, 다양한 공격도구에 의하여 중요한 정보가 유출되는 사고가 발생하기도 하였다. 이런 사례에서 볼 수 있듯이, 광대역을 보장하고 이기종망들이 통합되는 BcN 인프라를 기반으로 하는 미래 IT 환경에서는 경제, 사회, 국방 등 국가사회 전체에 치명적인 피해를 끼칠 수 있는 지능화된 사이버공격이 지속적으로 증가할 것으로 예상된다.

본 고에서는 이러한 통합 IT환경에서 우리가 직면할 정보보호 문제를 해결하기 위하여 BcN에 대한 주요 위협을 분석하고 이에 대한 정보보호 대응전략을 제안하였다. 본고의 정보보호 대응전략은 사이버 위협에 대한 정부, 기업, 개인의 정보보호 책임과 의무에 대한 인식, 그리고 그 실천이 병행될 때, 더욱 효과적으로 추진되어 안전한 u-Korea 구현을 위한 초석이 될 것으로 기대된다.

참고문헌

[1] 정보통신부, Broadband IT Korea 건설을 위한 광대역통합망(BcN) 구축 기본계획, 2004.

[2] 정보통신부, 정보보호 중장기 기술개발 로드맵, 2004. 7.

[3] 이병선, "NGN 구조의 국제표준화 동향," IT Standard Weekly, 39호, pp92-95, 2004. 10.

[4] ITU-T Recommendation X.805, "Security Architecture for Systems Providing End-to-end Communications", 2003.

[5] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements(3G TS 21.133 version 3.1.0)", 3GPP, 1999. 12

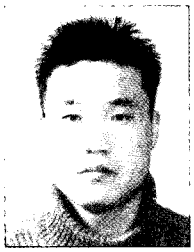
[6] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture", 3GPP, 2000. 10

[7] 한국전자통신연구원, 전자통신동향분석-광대역통합망 기술 특집, 통권 90호, 제19권 제6호, 2004. 12.

[8] 최병철, 김광식, 서동일, 장종수, "안전한 u-Korea 실현을 위한 정보화 역기능 방지 대책 - Security Belt", 전자통신동향분석 제20권 제2호, 2005. 4.

[9] ITU-T NGN FG Procedings Part 1, Part 2, 2005. (http://www.itu.int/ITU-T/ngn/)

저자약력



임 채 태

2000년 충남대학교 컴퓨터과학과(학사)
2003년 포항공과대학교 컴퓨터공학과(석사)
2003년-현재 한국정보보호진흥원 연구원
관심분야 : 정보보호, 이동통신, 네트워크
이 메 일 : chtim@kisa.or.kr

원 유 재

1985년 충남대학교 계산통계학과(학사)
1987년 충남대학교 계산통계학과(석사)
1998년 충남대학교 전산학과(박사)
1987년-2001년 한국전자통신연구원 책임연구원/팀장
2001년-2004년 안랩유비웨어/안철수연구소 CTO
2004년-현재 한국정보보호진흥원 팀장
관심분야 : 정보보호, 멀티미디어통신, 이동통신
이 메 일 : yjwon@kisa.or.kr