주 제

BcN과 보안 이슈

KT 이명수, 양재수

차 례

I. BcN 개요
II. BcN에서의 보안 위협과 대응방향
III. BcN 보안 솔루션
IV. 맺음말

I. BcN 개요

방송과 통신은 지난 100년 동안 서로 다른 영역으로 구분되어 서비스되어 왔으나, 최근에는 인터넷의 발달에 따라 서로의 영역에 대한 구분이 점차 모호해지고 있는 실정이다. 아울러 방송, 유선통신, 무선통신, 케이블 사업자들은 사업 영역의 확대를 위해 확장 가능하고 유연한 품질 보장형(QoS : Quality of Service) 네트워크를 원하고 있으며, 이러한 네트워크를 포괄적으로 차세대 통합 네트워크라고 한다. 한국에서는 정보통신부의 IT 839 전략의 3대 인프라 중의 하나인 BcN(Broadband converged Network)을 차세대 통합 네트워크로 볼 수 있으며, 미국, 일본, 중국 등도 광대역 멀티미디어 서비스를 제공할 수 있는 차세대 통합 네트워크 구축 전략을 세우고 있다.

BcN에서 필요로 되는 기술은 (그림 1)과 같이 크게 서비스, 제어, 그리고 전달 계층으로 나누어 볼 수 있다. 물론 전달계층 하부에 네트워크 액세스 계층과 서비스를 제공 받는 단말기 계층을 포함하여 고려할 수 있지만 망 통합관점에서 언급된 3개의 계층에 대해서 기술개발 요구사항만을 기술하고자 한다.

서비스 및 제어계층에서는 다양한 융합 서비스를 독립적으로 개발 수용할 것이기 때문에 유선통신, 무선통신 및 방송 통합을 위한 Open API 표준화 기술 및 상호운용성 기술과 XML 기반의 웹 서비스 기술, 네트워크와의 연동을 위한 시그널링 프로토콜 매핑 기술 등이 필요할 것이다. 또한 다양한 유, 무선 네트워크간 연결을 제어하고 음성과 멀티미디어 호 처리(call processing) 및 게이트웨이 제어를 위한 소프트 스위치와 같은 새로운 시스템 및 프로토콜의 개발을 요구할 것이다.

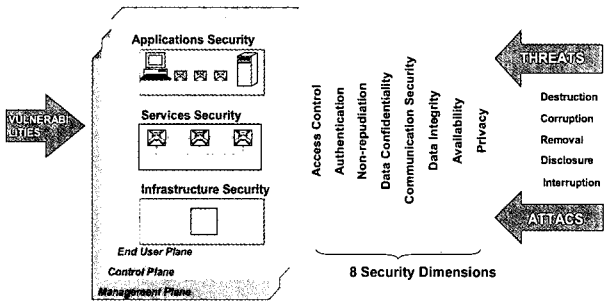
전달 계층에서는 새로운 BcN 융합 서비스를 제공할 수 있는 종단간(end-to-end) 맞춤형 품질 보장형 네트워크 기술이 요구될 것이다. 즉 품질 보장을 위한 QoS, MPLS 및 광대역 멀티서비스 제공을 위

한 FTTH(Fiber to the Home)등이 필요할 것이다. 또한 무선망, 방송망, USN망 등의 이종망간의 연동 및 통합을 위한 기술이 필요할 것이며, 다양한 IP망의 통합으로 인한 보안 문제를 해결하기 위해 다양한 보안 방안들이 연구될 것이다.

이러한 BcN 기술의 특징은 품질보장과 고속화로 크게 나누어 볼 수 있는데 이는 소비자에게 큰 편리함을 줄 수 있지만 반면에 지금 IP망의 위협이 더 신속하고 광범위하게 확산될 위험도 같이 가지고 있는 것이다.

II. BcN에서의 보안 위협과 대응방향

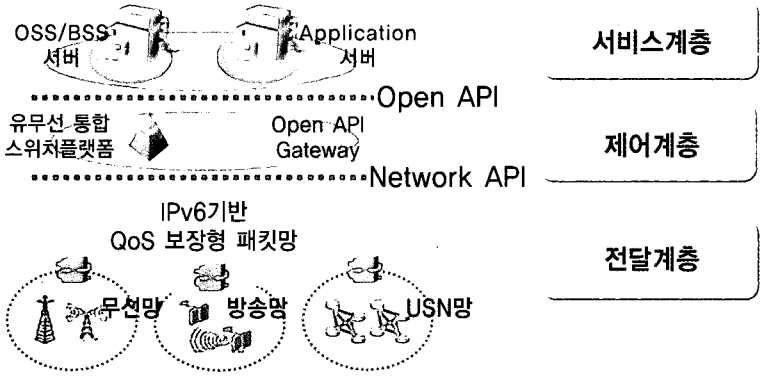
BcN에서 발생될 위협을 예상하는 것은 상당히 어려움이 따르게 되는데, 이것은 망의 통합으로 지금의 IP망의 위협들이 기존에 분리된 망들에 영향을 미칠 수 있을 것으로 생각되며, 그 피해 또한 클 것으로 예상되는 것에 반해서 고려해야 할 부분들이 너무 많으며 어떠한 형태의 공격이 나타날지 예측 불허라는 것이다. 여기서는 ITU-T에서 권고한 X.805를 기반으로 보호해야 할 부분들을 구분하고 그에 따른 보안 고려사항을 살펴본 후 좀 더 자세한 대응 기법을 언급하도록 하겠다.



(그림 2) 종단간 네트워크 보안을 위한 X.805 보안 아키텍처

01. X.805 보안 아키텍처

ITU-T의 X.805는 '종단간 통신을 제공하는 시스템에 대한 보안 체계' (Security architecture for systems providing end-to-end communications)라는 제목으로 얼핏 보면 BcN과 거리가 있어 보이지만 종단간 통신을 위한 보안 체계라는 것은 모든 네트워크에서 최종적으로 구현되어야 할 보안 체계라고 생각할 때 BcN에도 기본적으로 구현되어



(그림 1) BcN 개념도

야 할 체계라고 볼 수 있다. 또한 이 권고안은 ITU-T에서 BcN 표준화를 다루는 FGNGN(Focus Group NGN)의 WG 5(Working Group 5)인 SeC (Security Capability) Group에서 나온 것으로 향후 BcN의 보안 체계에 대한 기반이 될 것이다. X.805에서는 보안 디멘전(SD: Security Dimension), 보안 계층(SL: Security Layer)과 보안플레인(SP: Security Plane)으로 나누어 외부 위협에 대한 보안 체계구축 방안을 제시하였다.

보안 디멘전

액세스 제어: 네트워크 자원의 적합한 사용으로 권한 있는 사용자나 장비만이 네트워크 자원이나 서비스 및 애플리케이션에 접속하도록 허용한다. 여기에는 패스워드나 접근제어 목록(ACL: Access Control List)과 같은 기법들이 포함될 수 있으며 이를 통해 불법적인 접근을 차단한다.

인증(Authentication): 통신하는 상대편의 신원을 확인하는 것이며 이를 통해 다른 사람으로 가장(masquerade)하여 정보를 빼내려는 행위를 방지한다. 여기에는 PKI, 전자인증서 등이 포함된다.

부인거부(Non-repudiation): 네트워크에서 행해진 활동들에 대해 나중에 부인하지 못하도록 하는 증거를 만드는 것으로 시스템 로그, 전자 서명 등이 포함될 수 있다.

데이터 기밀성 : 자료의 기밀성을 유지하는 것으로 암호화 기법이 포함될 수 있다.

통신(Communication) : 통신이 오직 발신자와 수신자 두 사람 사이에서만 일어나도록 하는 것으로 통신 흐름을 가로채거나 우회시키는 것을 방지하는 것이다. 여기에는 L2TP, VPN, MPLS와 같은 기술들이 사용된다.

데이터 무결성(Data Integrity) : 자료의 전송 혹은 저장 중에 비 권한적인 변조, 삭제, 생성 그리고 복사로부터 보호하는 것으로 여기에는 MD5, 전자서명 등이 포함될 수 있다.

가용성(Availability) : 네트워크 자원, 서비스 그리고 애플리케이션을 합법적인 사용자들이 필요한 때에 사용할 수 있게 하는 것으로 여기에는 재난 복구(DR : Disaster Recovery)기법이 포함된다.

개인정보보호(Privacy) : 네트워크 활동에 대한 무분별한 모니터링으로부터 사적인 개인비밀을 지키는 것이다.

보안계층

보안계층(security layer)은 아래와 같이 3개로 나누어지며 기반 구조(infrastructure)를 토대로 응용(application)을 통해 사용자들에게 서비스하는 일련의 통신서비스체계를 모델로 하였다.

기반구조(Infrastructure) : 네트워크 서비스나 애플리케이션들을 위한 전송 장비들이나 개별 네트워크를 위에서 언급한 Security Dimension들을 고려해 보호한 기반 구조 계층이다.

서비스 : 서비스 제공자가 그들의 고객들에게 제공하는 서비스들의 보안에 대한 계층이다.

응용 : 고객들에 의해서 접근되는 네트워크 기반의 응용에 대한 보안을 고려하는 계층이다.

보안 플레인

보안 플레인(Security Plane)은 아래와 같이 3개로 나누어 지며 그림 10.2에 보는 것처럼 각각의 Plane들은 기반 구조 보안계층(Infrastructure Security Layer), 서비스 보안계층(Service Security Layer), 응용 보안계층(Applications Security Layer)으로 구성된다.

관리(Management) : 네트워크 자원, 서비스 그리고 애플리케이션의 관리와 공급에 관련된 것으

로 네트워크의 운영에 필요한 보안을 고려하는 영역이다.

제어(Control) : 네트워크가 효율적으로 정보를 전송하고 애플리케이션을 서비스할 수 있게 하는 활동들에 대한 보안과 연관된 영역이다. 유해 트래픽에 대한 차단이나 탐지가 여기에서 고려될 수 있다.

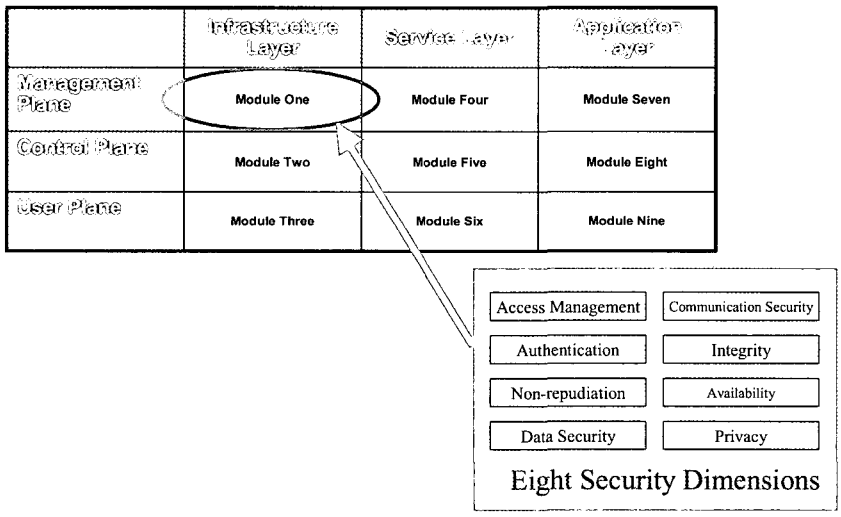
최종 이용자(End-User) : 다양한 목적을 가진 고객들의 네트워크 접근에 대한 보안을 고려하는 영역이다. 개인 프라이버시 문제와 저작권 문제와 같은 사항들이 여기에서 고려될 수 있다.

02. X.805 기반 BcN 보안 유형

(그림 3)은 기반구조(Infrastructure) 계층(layer)의 관리 플레인에서 8개의 보안 디멘전에 대해 생각해 보는 것이다. 8개의 보안 디멘전중 액세스 제어에서는 적합한 사용자 및 장치만 네트워크 장비에 대한 관리 활동을 수행할 수 있게 해야 한다는 것이다. 또한 개인정보 보호와 같은 경우 네트워크 장치 식별 및 통신 정보가 비 권한자에게 노출되지 말아야 한다는 것이다. 이렇게 9개의 영역을 나누어서 그 분야에서 8개의 보안 디멘전에 대해 생각한다는 것은 복잡하고 많은 보안 고려 사항을 체계적으로 나누어 생각해 볼 수 있는 좋은 표준이라고 생각된다. 예를 들면 BcN의 경우 다양한 포트사용과 세션을 사용한 서비스들로 기존의 보안 장비로 민감한 서비스들을 보호하는 데는 한계가 있을 수 있는데 이러한 문제의 경우 서비스 계층의 제어 플레인 중에 가용성 보안 디멘전에서 고려해야 할 사항이라고 볼 수 있는 것이다.

기반구조 계층, 관리 플레인

서비스 게이트웨이에서의 신뢰성을 보장하는 문제, 소프트스위치 자체의 신뢰성을 보장하는 문제, 그리고 이종망간의 상호 연동 관리 문제가 여기에 포함될 수 있다. 서비스 게이트웨이나 소프트스위치의 신뢰성 보장 문제는 이중화로 어느 정도 신뢰성을 확보할 수는 있겠지만, 이는 어디까지나 운영상의 에러에 대한 방안이지 악의적인 공격에 대한 대응 방안이 아니다. 이러한 악의적인 공격에 대응하기 위해서는 침



(그림 3) X.805 기반 BcN 보안 유형

입차단시스템(IPS)과 같은 보안장비가 필요한데, 문제는 이러한 보안장비의 처리능력이 전체 백본 인프라의 처리 능력에 비해 많이 떨어진다는 것이다. 즉 서비스 게이트웨이나 소프트스위치의 생존성을 보안장비로 확보한다고 할지라도 전체 백본 인프라의 생존성에 대한 보호방안이 없다면 서비스는 또 다시 1.25대란과 같은 사태로 정지될 수 있는 것이다. 아울러서 패스워드의 복잡성이나 인증서 기반의 인증과 같은 강력한 인증 제어 체계, 관리자들의 작업 내역 관리, 시스템의 로그 관리, 중요 데이터의 암호화, 재난 복구 체계를 통합적으로 갖추어야 할 것이다. 시스템의 IP나 DNS 서버의 위치와 같은 주요 관리 정보는 따로 보관하며 그러한 자료에 대한 접근은 적절한 방법으로 통제되어야 한다.

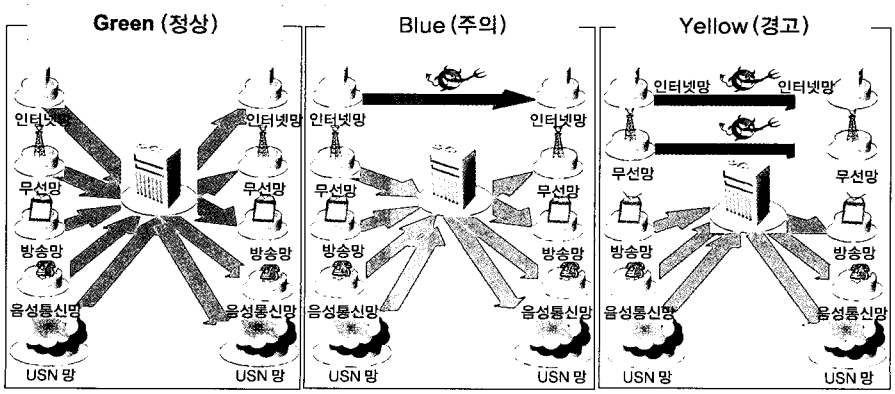
이종망간의 상호 연동에 대한 관리 문제의 경우 BcN는 유선, 무선, 방송망 등 다양한 망들이 통합되므로 유선 망의 장애가 다른 무선, 방송 및 PSTN망에 영향을 미칠 수 있게 될 것이다. 그래서 PSTN을 연결해주는 트렁크(Trunk) 게이트웨이가 악의적인 공격으로 장애가 발생했을 경우 일반 음성 통신이 되지 않는 최악의 사태가 일어날 수 있을 것이다. 차라리 연동하지 않고 서비스하는 것만 못할 경우가 발생하는 것이다. (그림 4)의 망 분리 방안과 같은 방법이 좋은 예가 될 수 있다고 생각된다. BcN의 상태를 Green, Blue, Yellow로 나누고 이종 망에서 문제가 발생할 경우 그러한 문제를 신속히 탐지하고 차단함으로써 나머지 망의 가용성을 확보하는 것이다.

기반 구조 계층, 제어 플레인

소프트스위치 제어 정보 보호 및 서비스 게이트웨이 제어 정보 보호는 소프트스위치가 호를 연결해 주기 위해 사용하는 제어 신호를 안전하게 보호하는 방안으로 주요 신호 패킷에 대한 인증 및 암호화를 통해 이를 구현할 수 있다.

기반구조 계층, 이용자 플레인

여기서는 전송되는 가입자의 정보를 보호하는 문제, 위장 단말기를 탐지해야 하는 문제, 그리고 가입자 장비에서 발생하는 정보보호의 취약성 문제를 들 수 있다. 특히, 가입자 장비 중 USN(Ubiquitous Sensor Network)에 사용되는 장비들은 저 용량의 CPU및 메모리를 가질 것으로 예상되며 전파방해와 같은 DoS성 공격에 의해 쉽게 무력화 될 것으로 보인다. 불행하게도 이에 대한 대책은 장비의 특성상 쉽지



(그림 4) 망 분리 방안

않을 것으로 예상된다.

전송되는 가입자 정보 보호는 TLS와 같이 신뢰된 암호화 전송 프로토콜을 사용함으로써 해결할 수 있으며 위장 단말기 탐지를 위해서는 강력한 인증 및 추적 시스템이 사용될 수 있을 것이다. 익명성을 원하는 인터넷 사용자의 요구는 BcN에서도 계속 이어질 것으로 보이며 이에 따라 악의적인 사용자를 추적하는 것은 용이하지 않을 것으로 보인다. 따라서 하니 팟(honey pot)이나 하니 넷(honey net), 그리고 포렌식(forensic) 같은 기법의 적용을 적극 고려해 보아야 할 것이다.

다른 방안으로 검역 네트워크를 고려할 수 있다. 검역(quarantine) 네트워크란 가입자 단말이 네트워크에 접속하는 단계에서부터 가입자 단말의 보안 상태를 점검하여 격리, 치료, 접속허용 등 일련의 보안 조치를 취하는 네트워크로서 가입자와 통신망을 동시에 보호하는 것을 그 목적으로 하고 있다.

대개의 통신망 회사는 수 만개에서 수십 만개까지 많은 수의 가입자 장비들을 가지고 있기 때문에 그 운영 및 보안 관리에 어려움을 겪고 있는 실정이다. 가입자 장비의 정보보호 취약성은 다양한 서비스의 개발과 함께 더욱 증가할 것으로 보이며 무선 장비의 경우 메모리나 CPU가 유선 장비에 비해 성능이 떨어지기 때문에 복잡한 암호화 기법이나 고성능을 요구하는 보안 기술이 적용될 수 없을 것으로 보인다. 이에 따라 서비스 개발 시에는 보안성 평가를 반드시 받도록 하고 사용자들에 대한 정보보호 교육을 강화하도록 한다.

서비스 계층, 관리 플레인

서비스 계층에 대한 관리 문제와 서비스에 대한 인증 문제가 이 부분에 포함된다. BcN에서는 서비스별로 과금이 이루어질 것으로 보이며 과금의 방식도 사용자가 사용한 시간을 근거로 하는 방식에서 패킷 단위의 과금까지 다양한 방식이 도입될 것으로 보인다. 이러한 과금 정보가 별도의 망이 아닌 일반 데이터 망으로 전송될 경우 공격자들은 이러한 정보를 변경하거나 손상시킴으로써 서비스를 공짜로 이용하고자 시도할 것이다. 따라서 서비스계층의 관리 권한은 다양한 서비스를 중앙 집중적으로 통합해서 관리 할 수 있는 통합 보안 관리시스템의 개발 및 적용을 고려해야 할 것이다.

서비스 인증은 사용자들에 대한 차별화된 서비스 제공 및 과금을 위해서 USB인증 및 생체 인식과 같은 강력한 인증 기법을 도입하도록 한다. 최근에는 핸드폰으로 변경된 패스워드를 보내주는 방법도 상용화되어 증권거래에 이용되고 있다. 이 경우 패스워드가 수시로 바뀌고 충분한 복잡성을 가지면서도 사용자만 볼 수 있도록 함으로써 거래의 안정성을 높일 수 있다.

서비스 계층, 제어 플레인

검증되지 않은 서비스 제공으로 인한 제어권의 상실 문제와 서비스 품질 보장 문제가 여기에서 생각될 수 있다. 서비스 품질 보장에 가장 큰 위협은 분산서비스거부공격(DDoS)이 될 것으로 보인다. BcN에서 화상전화는 품질에 민감한 서비스가 될 것으로 보이며 이 경우 일반적인 서비스거부공격(DoS) 공격에 의해서도 서비스의 품질이 크게 영향을 받을 수 있다. 따라서 라우터의 ACL을 통한 차단기법, Ratelimit 기법, uRPF (unicast Reverse Path Forwarding), 블랙홀 기법을 통해 이러한 영향을 미리 차단하거나 완화시키도록 한다. 또한 검증되지 않은 서비스의 무분별한 사용은 분산서비스거부공격의 진원지가 될 수 있으므로 새로운 서비스의 개발 시에는 반드시 보안 평가 과정을 거치도록 한다.

서비스 계층, 이용자 플레인

서비스 사용자의 개인 정보보호 문제와 불건전 정보 및 반사회적 정보의 유통 문제가 이 분야에서 고려될 수 있다. 최근 인터넷을 이용한 금융사기와 사고가 잇따르고 있는데, 대표적인 공격기법인 피싱(Phishing)과 파밍(Pharming)을 예로 들 수 있다. 요즘에는 피싱보다 진보된 파밍이란 공격이 현저하게 나타나고 있다. 파밍은 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 DNS 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도하여 개인정보를 훔치는 새로운 수법인데, 기존 피싱 공격과는 달리 파밍은 아예 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 중간에서 탈취하기 때문에 사용자들은 늘 이용하는 사이트로 알고 의심 없이 개인의 인증번호, 비밀번호 및 신용카드 번호 등을 입력하게 되고 이는 그대로 공격자에게 전송되게 된다. BcN에는 PSTN 망도 같이 연동되기 때문에 인터넷 뱅킹뿐만 아니라 폰 뱅킹도 위와 같은 공격의 대상이 될 위험이 있다.

응용 계층, 관리 플레인

개방형 API제공으로 인한 취약점의 증가로 인한 문제가 여기에서 논의 될 수 있다. 웹 사이트를 개설하다 보면 공개 게시판 프로그램을 설치하게 되는 경우가 종종 있는데, 이러한 게시판 프로그램의 취약점을 이용한 해킹 프로그램들이 존재하고 피해 사례도 볼 수 있다. 한국정보보호진흥원(KISA)는 국산 공개 웹 게시판 프로그램인 '제로보드'의 취약점을 이용해 2,300여 개에 달하는 홈페이지들을 변조하는 사건이 발생했다고 발표했고 '주의' 경보를 발령했으나, 보안 패치를 위한 제작자를 찾지 못해 어려움을 겪었다고 한다. 공개 SW의 속성상 제작자들의 연락처를 알아내는 것이 어려웠고 이에 따라 제로보드를 사용하는 개별 기업들에게 일일이 연락해서 패치 할 것을 권유해야 했는데, 대부분의 업체가 웹 호스팅 등 외주로 홈페이지를 관리하고 있어서 자사의 홈페이지가 어떤 SW로 제작됐는지조차 모르는 경우가 많았다고 한다. 2004년 10월에는 브라질 해커그룹이 또 다른 공개 SW인 '테크노트' 게시판 프로그램의 취약점을 이용해 200여 개의 국내 홈페이지를 변조하는 사건도 있었다. 이처럼 공개 SW의 취약점은 다수의 프로그래머들이 연속적으로 제작과 패치에 참여하는 공개형 제작 방식으로 인해 적기 적소에 버전 패치가 이루어지기 힘들다. 또한 인터넷으로 불특정 다수가 언제라도 다운 받아 사용할 수 있기 때문에 누가 이들 프로그램을 사용하는지 파악하기도 쉽지 않다. 이 때문에 이들 프로그램의 보안 패치가 이루어지더라도 이를 사용자들에게 통보하고 패치 시킨다는 것 자체가 어려운 일이며, 여전히 패치 되지 않은 시스템이 어딘가에 존재하게 되는 것이다.

BcN도 이러한 문제로부터 자유로울 수 없으며 취약점이 발견된 API를 많은 애플리케이션에서 사용한다면 그 문제는 확대될 수 있다. 이에 대한 대응 방안으로 최신 버전으로의 지속적인 패치를 많이 권하는데 관리하는 애플리케이션의 수가 적다면 어느 정도 가능할 지 모르나 그 규모가 클 경우 일일이 패치 한다는 건 어려운 일이다. 또한 패치로 인한 서비스 중단과 패치 이후 서비스에 이상이 생길 수 있다는 걱정 때문에 관리자들이 사고가 일어나지 않는 한 패치를 잘 하지 않는 수동적인 자세도 그러한 어려움을 가중시킨다.

응용 계층, 제어 플레인

검증되지 않은 애플리케이션의 사용으로 인한 제어권의 상실 문제를 들 수 있는데, 이 부분은 여러분들의 컴퓨터에 있을지 모르는 웜 바이러스가 대표적인 예라고 할 수 있을 것이다. 2001년 4월 미국정찰기와 중국전투기의 충돌 사태로부터 야기된 사이버

전쟁이 있었다. 이때 사용됐던 취약점이 2000년 10월에 발표된 IIS UNICODE 보안 취약점으로, 웹 서버를 마이크로소프트의 IIS 4.0 혹은 5.0을 사용하고 있을 경우 원격 사용자가 임의의 명령어를 인터넷 익스플로러 주소 창에 입력하여 대상 호스트에 접속하면, 서버 자체에 명령을 내릴 수 있는 취약점이었다. 이 취약점을 이용하면 취약점을 가지고 있는 대상 호스트의 모든 파일을 생성 · 수정 · 삭제할 수 있으며, 미국과 중국의 해커들은 이를 이용해 서로의 정부를 비방하는 글로 서로의 홈페이지를 변조시켰다. 사이버 전쟁이 진행되고 있을 때 이 취약점은 웜 바이러스로 제작돼 국내외 많은 서버와 클라이언트 PC를 감염시켰는데, 그것이 바로 코드 레드(Code Red)와 님다(Nimda) 웜 바이러스이다.

한편 1.25대란으로 불리는 슬래머 웜 바이러스는 MS의 데이터베이스인 MS-SQL 서버의 취약점을 이용한 것으로 MS-SQL 서버를 감염시키고 클라이언트 PC를 재감염 시켰다. 대다수의 서버와 클라이언트 PC가 감염되면서 네트워크 트래픽이 폭주했고, 그 결과 국내의 DNS서버의 서비스 장애를 가져왔고 전체 네트워크가 마비되었다. 이로 인해 많은 전자상거래업체, 공공기관, 일반 기업, PC 방 등이 엄청난 손실을 입었다.

응용 계층, 이용자 플레인

지적 재산권 보호 문제가 여기에 포함될 수 있다. 2001년 1월 16일 MP3 파일의 공유 툴을 제공하는 소리바다에 대해 4개 음반회사가 저작권 침해로 고소한 것을 시작으로 디지털 지적 재산권에 대한 의식이 변화하고 있다. 예전에는 인터넷에 올라오는 일반인들의 글을 출처확인과 작성자의 허락 없이 가져가는 일이 빈번했고 문제가 되더라고 간단히 사과함으로써 해결되었다. 하지만 지금은 디지털 컨텐츠에 지적 재산권이 부여되고 법적으로 보호되고 있다. 문제는 지적재산권이 법과 같은 제도만으로는 보호되지는 않는다.

III. BcN 보안 솔루션

BcN에서는 보안의 범위가 개인 컴퓨터 혹은 지역망 등의 소규모 네트워크가 아닌 대규모 네트워크로 확대될 것이다. 확대된 보안 범위를 커버하고 기존 네트워크 보안의 문제점을 해결하며, 새롭게 등장하는 미래형 네트워크인 BcN에 맞는 효율적이고 관리가 용이한 방식의 차세대 네트워크 보안이 요구된다고 할 수 있다. 이를 위해 현재 네트워크 보안 기술 개발의 동향을 반영한 BcN에 적용할 수 있는 몇 가지 보안 솔루션들을 살펴본다.

01. 네트워크 보안 기술 개발 동향

네트워크 보안 기술은 보안 기능별로 개별 제품을 생산하던 형태에서 통합 보안 형태의 제품으로 발전해 나가고 있다. 통합 보안 형태는 하나의 플랫폼에 다양한 보안 기능을 통합함으로써 기존에 개별적으로만 다루었던 보안 기능들을 서로 통합 및 연동하여 부가적인 이점을 이끌어내고 있으며, 보안 기능의 개별적 관리에 따른 관리자의 부담을 감소시켜 준다는 장점을 가진다. 이러한 통합 추세는 소프트웨어뿐만 아니라 하드웨어에서도 일어나고 있는데, 기존의 네트워크 장비 업체들이 보안 기능들을 탑재하여 제품들을 출시하고 있는 데서 그러한 경향을 알 수 있을 것이다. 이렇게 장비에 탑재되는 보안 기능들은 대부분 전용 칩을 탑재하여 네트워크의 고속화 추세에 따른 성능 향상을 꾀하고 있다. 이에 따라 기존의 보안 장비가 메가급 트래픽을 처리하는 성능을 보이는 것에 비해 최근에 출시되고 있는 보안 장비는 기가급 트

래픽을 처리하는 성능을 가지고 있다.

보안 제품의 다양화는 관리상의 어려움을 증가시키고 있으며, 이에 따라 많은 보안 제품들을 자동적으로 관리하고 제어할 수 있는 정책기반의 통합적 관리 메커니즘이 요구되게 되었다. 이러한 통합 관리 메커니즘 기술을 구현한 제품은 다양한 보안 제품들을 자동적으로 관리하고 제어할 수 있도록 하며, 보안 정책에 따른 일관성 있는 관리를 도와 준다. 이러한 보안 정책은 IETF나 DMTF(Distributed Management Task Force)에서 추진되고 있는 표준화를 따르고 있다. 이기종 보안 제품간 상호연동을 위해 표준 프로토콜 또한 개발되고 있는데, 체크포인트사가 주도하고 있는 OPSEC(Open Platform for SECurity)이나 IETF에서 진행중인 IDMEF(Intrusion Detection Message Exchange Format)등이 대표적인 예이다. 아울러 해커들의 네트워크 침입에 대하여 기존의 관제 시스템을 통해 대응하는 수동적이며 방어적인 네트워크 보안 기술에서 탈피하여, 침입자를 경로를 역추적하여 계속적인 침입을 막기 위한 능동적이고 지능적인 네트워크 보안 기술 또한 요구되고 있다.

02. 하드웨어 기반 솔루션

보안 라우팅 장비: 장비 업체들은 자사의 네트워크 장비에 방화벽, VPN, 침입탐지, 컨텐츠 필터링 기능을 하드웨어 기반으로 제공하고 있다. 라우터 장비 업체인 주니퍼가 방화벽 전문 업체인 넷스크린을 인수한 것은 이러한 시장의 추세를 반영한다고 볼 수 있다.

침입방지시스템(Intrusion Prevention System): 잠재적 위협을 인지한 후 즉각 대응을 하는 예방적 차원의 보안 시스템으로 LG 엔시스, Network Associates, Tipping Point, 시큐아이닷컴, 정보보호기술, 포티넷 코리아, 라드웨어, ISS, 탑레이어 네트웍스등 많은 업체들이 1Gbps에서 4Gbps 처리 용량을 가지는 침입방지시스템을 시장에 선보이고 있다.

통합보안 관리 시스템(Enterprise Security Management): 보안장비에 대한 보안정책 적용, 침해 유형 모니터링과 같은 목적으로 사용되는 시스템으로 여러 곳에 분산된 보안 시스템과 네트워크 장비를 중앙센터에서 제어하거나 감시한다.

침입감내 시스템(Intrusion Tolerant System): 기존의 보안 장비들은 침입의 방지와 탐지에 중점을 두고 개발된 반면, 침입감내 시스템의 경우에는 침입이 성공하였다 하더라도 시스템의 중요 서비스의 지속적인 제공을 목표로 연구 개발되고 있는 보안 시스템이다.

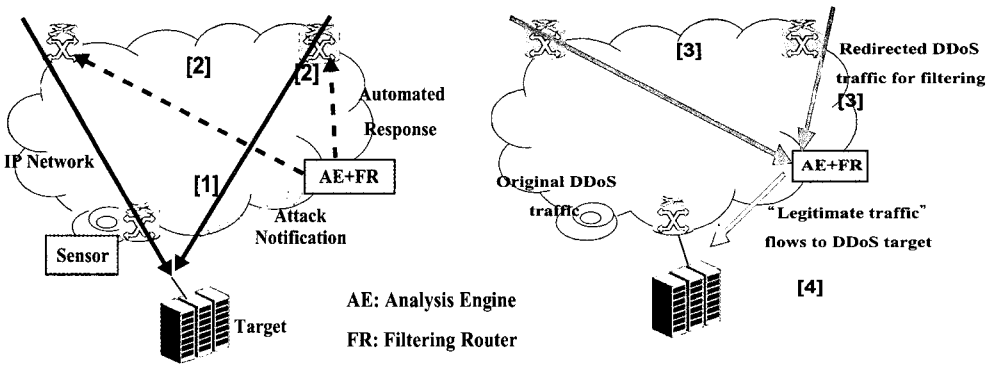
조기경보 시스템: 조기 경보 시스템이란 조직의 업무 연속성을 위해 위협 요인을 사전에 탐지 및 식별하여 피해를 예방하는 것을 말한다. 조기 경보 시스템의 구성 요소로는 트래픽을 감시하고 분석하는 트래픽 분석 시스템, 어떤 특정 이벤트 발생시 이의 분석을 위한 이벤트 분석 시스템, 사전 예방을 위해 시스템의 취약성을 수집하기 위한 취약성 수집 시스템, 그리고 침해 발생시 신속한 대응을 위한 전파 및 발령 시스템이 있다.

03. DDoS 완화 기법

품질 보장형 네트워크 서비스를 제공하는 BcN에서는 DDoS 공격에 의한 네트워크 자원의 고갈은 현재의 네트워크에 대한 피해보다 더 많은 손실을 가져올 것이다. 이에 따라 BcN에서는 DDoS 공격에 대한 대응 기법이 중요한 역할을 할 것으로 기대된다.

DDoS 공격의 완화 기법 중 하나로 Arbor Networks Peakflow SP를 들 수 있다.

Arbor Networks Peakflow SP는 (그림 5)와 같



(그림 5) DDoS 완화 기법

이 동작하여 DDoS 공격을 완화시킨다.

자세한 동작 순서는 다음과 같다.

[1] 공격 대상의 라우터에 위치한 센서에서 DDoS 트래픽을 감지하여 공격이 일어나고 있음(Attack notification)을 AE(Analysis Engine)+FR(Filtering Router)에 알린다. AE+FR은 트래픽을 분석하고 트래픽의 진입 지점을 찾는다.

[2] AE+FR은 트래픽 진입 지점의 라우터에게 트래픽을 공격 대상에서 AE+FR로 흐르도록 트래픽 경로를 변경시킨다.

[3] AE+FR로 DDoS 공격성 트래픽이 흐르기 시작한다.

[4] AE+FR에서 DDoS 공격성 트래픽은 걸러지고 정당한 트래픽만이 흐르게 된다.

이와 같은 DDoS 완화 기법은 기존의 망 구성을 크게 변형시키지 않기 때문에 효율적이라고 볼 수 있는 반면 라우터의 경로 설정을 바꿔야 하는 어려움이 있다.

04. 능동형 보안 관리 기법

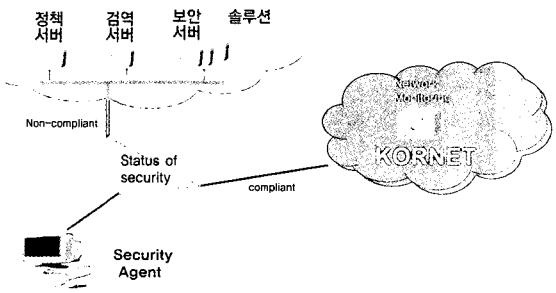
능동형 보안 관리 기법이라는 것은 공격 기법의 고도화에 따라 네트워크 인프라 차원에서 실시간 침입에 대한 탐지 및 역추적, 복구 등의 기능을 효율적으로 수행할 수 있는 네트워크 차원의 보안 기술을 일컫는다. 미국의 경우 네트워크 보안과 생존성 향상을 위해 DARPA(Defense Advanced Research Projects Agency) ITO(Information Technology Office)에서 안전한 네트워킹(Secure Networking)과 관련한 연구를 진행하고 있으며, 스위스, 네덜란드, 핀란드 등 유럽의 경우에도 컨소시엄 형태로 10개국이 참여하는 FAIN (Future Active IP Network) 프로젝트에서 이와 관련한 연구를 수행하고 있다.

이러한 연구는 피해 네트워크의 경계에서 해당 공격자의 트래픽을 차단하는 것이 아니라, 공격자의 실제 위치를 역추적하고 공격자의 네트워크에 대한 접근성을 차단함으로써 고립화시키는 보다 강력한 대응을 수행하는 네트워크 보안 프레임워크를 구축하는 것을 목적으로 한다. 능동형 보안 관리 프레임워크는 지능형 정보보호 기능의 탑재, 네트워크의 전반적

인 협업관계와 관련 기능의 실시간적 활성화, 네트워크로부터의 공격자 단절 기능 제공, 적응성을 지니는 보안 플랫폼 제공, 시스템 및 서비스간의 상호연동 관계 향상 기능들을 포함함으로써 그 목적을 달성하고자 한다.

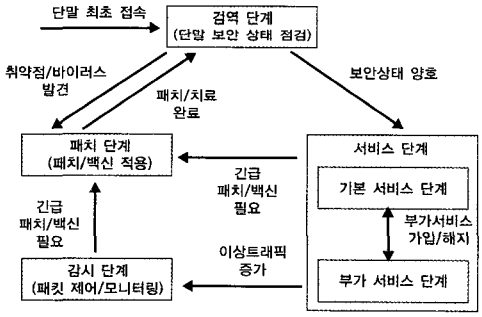
05. 검역(Quarantine) 네트워크

검역 네트워크란 가입자 단말의 보안 상태를 점검하여 격리, 치료, 접속허용 등의 조치를 취하는 네트워크로서 문제가 될 소지를 사전에 예방하고자 하는 개념의 네트워크이다. 검역 네트워크는 일반적으로 (그림 6)과 같이 구성된다. 정책 서버는 망 사업자의 접속 정책 및 보안 정책을 관리하며, 검역 서버는 가입자 단말 및 네트워크의 보안 상태와 보안 정책에 따라 격리, 치료, 접속허용 등의 조치를 지시하는 서버이다. 보안 솔루션서버는 바이러스 진단, 치료 및 보안 패치 다운로드 등과 같은 보안 서비스를 제공해주고 네트워크 접속 시스템은 보안상태 점검 결과에 따라 가입자 단말의 네트워크 접속을 제어한다. 가입자 단말에는 가입자 단말의 보안 상태 점검을 위해 보안 에이전트가 가입자 PC에 설치된다.



(그림 6) 검역 네트워크

(그림 7)은 검역 네트워크 동작 방식을 설명해 준다. 가입자 단말이 네트워크 접속을 시도하면 검역 서버에서 단말의 보안상태를 점검한다. 만약 보안 상태가 망의 접속 정책 및 보안 정책에 부합하면 서비스 단계로 이동하여 정당한 서비스를 제공받는다. 그러나 웜 바이러스에 감염되었거나 패치되지 않은 등의 취약점이 발견 되면 검역 서버에 의해 격리되어 보안 솔루션 서버에 의해 패치 및 치료를 받는다. 치료를 마친 단말은 정상적인 네트워크 접속이 허용되어 정상적인 서비스를 받게 된다. 서비스를 받고 있는 서비스 단계라도 이상 트래픽이 증가되면, 감시단계로 전환하여 관련 단말을 파악하고 해당 단말에 대한 격리 조치 및 치료를 수행하게 된다.



(그림 7) 검역 네트워크의 동작 방식

위에서 본 보안 솔루션들은 현재 상용화 되었거나 연구 개발중인 솔루션으로 기존 네트워크 운영에 따라 요구되고 있는 보안 기능들이다. 따라서 향후에는 BcN의 운영에 따라 새롭게 요구되는 보안 기능들이 있을 것으로 예상되지만, IP망을 기본적으로 사용한다면 그 차이는 크지 않을 것으로 생각된다. 네트워크 장비에 보안 기능이 기본적으로 추가됨으로써 이제는 보안과 네트워크관리가 따로 구분되어 이루어지지 않을 것이며 문제는 이러한 보안 기능들을 어떻게 효율적으로 연계하여 위협에 대처할 수 있겠는가가 중요 관심거리가 될 것이다.

IV. 맺음말

지금까지 BcN에서 예상되는 위협과 그에 대한 대응 방향을 ITU-T의 X.805에 제시된 영역으로 나누어 살펴보았다. 이러한 검토를 통해 아래와 같은 부분들이 BcN에서 고려되어야 할 것이라고 생각된다.

보다 영리하고, 지능적이고, 능동적인 통합보안시스템이 필요하다.

침입차단시스템의 보안 정책은 주로 네트워크 주소와 프로토콜 정보들로만 운용되고 있기 때문에 세밀한 차단이 어렵다. 또한 일반적으로 침입차단시스템은 패킷이 시스템을 통과하는 동안 패킷을 일일이 검사하게 되어 있어 데이터 처리량을 감소시킬 뿐 아니라 네트워크 병목이 될 수 있다. 침입탐지 시스템의 경우에도 정의되지 않은 패턴의 유입과 다양한 우회 기법 등에 의한 오동작 확률이 크다. 그러므로 더욱 다양하고 많은 공격이 예상되는 BcN에서는 침입탐지시스템기능, 침입차단시스템기능, 가상 사설망 기능(VPN)등이 통합되어 예상되는 공격에 보다 신속하게 대응할 수 있어야 한다. 또한 인라인 보안장비에 문제가 발생할 경우 L2스위치 기능이 동작하여 정상 동작에 미치는 영향을 최소화하는 바이패스(bypass)기능도 가용성 측면에서 필요할 것으로 보인다.

보다 강력한 인증, 권한, 추적 기능이 필요하다.

기존의 아이디/패스워드(ID/PW)방식의 인증 및 권한 부여는 여러 문제를 안고 있으며 해킹의 가장 기본적인 공격 대상이 되곤 한다. 따라서 BcN에서는 PKI, 생체 인식과 같은 강력한 인증, 역할 기반 접근 제어 (RBAC: Role Based Access Control)를 통한 권한 부여 그리고 Forensic 기술을 통한 감사 및 추적 기능의 강화가 필요하다.

새로운 서비스 개발을 위한 보안 지침 및 검토 방안이 필요하다.

BcN는 다양한 서비스 제공을 위해 필요한 하부 구조이다. 따라서 다양한 서비스의 개발이 이루어질 것이고 그에 따른 보안 지침이 없다면 무분별한 서비스 개발에 따른 보안 취약점의 증가는 피할 수 없는 결과를 야기시킬 것이다. 기존의 ISO 17799나 BS7799와 같은 보안 평가 표준이 있기는 하지만 이는 기존의 시스템에 관한 일반적인 표준으로 BcN에 적용하기에는 부족한 면이 있다. 따라서 BcN를 위한 보안 지침 및 기준이 필요하다.

알려지지 않은 공격에 대한 대응 방안 수립이 필요하다.

하니 팟(honey pot)으로 알려진 가장 공격자 유인 시스템은 새로운 공격의 유형을 파악할 수 있는 기법이다. 또한 anomaly detection 기법은 기존의 네트워크 패턴과 다른 네트워크 패턴이 감지될 경우 이를 알려주어 알려지지 않은 공격이 일어나고 있는지에 대한 경고를 해 줄 수 있는 기법이다. 이와 같은 조기 탐지 체계를 통해 차세대 네트워크에 일어날 수 있는 알려지지 않은 공격을 완화시킬 수 있어야 한다.

중앙 집중된 통합 보안 관리 체계가 필요하다.

조기 탐지 체계를 통해 공격을 신속하게 탐지한다고 하더라도 이에 대한 차단 조치를 취할 수 없다면 아무런 소용이 없다. 따라서 중앙 집중된 통합 보안 관리 체계를 통해 BcN에 문제가 발생시 이를 신속하게 차단하고 정확한 문제점을 파악하여 향후에 그런 문제로 인해 망의 가용성이 영향을 받지 않아야 한다.

좀 더 강화된 개인정보 보호 기술이 필요하다.

BcN의 사용자들은 다양한 단말과 서비스들을 이용하게 될 것이다. 이에 따라 사용자들은 지금보다 많은 불건전 정보를 다양하게 접하게 될 것이다. 따라서

이러한 불건전 정보를 자동적으로 선별하고 분류하여 차단할 수 있는 기술이 제공되어야 할 것이다. 또한 방송, 통신의 융합 하에서 방송 컨텐츠에 대한 저작권 보호, 불법 복제를 방지할 수 있는 컨텐츠 보호 기술도 강화되어야 할 것이다.

보안 위험발생 수준에 따른 단계적 망 분리방안이 필요하다.

무선, 유선, 방송, 전화망과 같은 이기종 망들이 통합되어 있는 BcN의 경우 위험발생을 신속히 파악하고 그 원인을 통합 네트워크에서 분리할 수 있는 구조를 고려해야 한다. 이는 다른 망의 생존성을 확보하고 피해를 최소화 할 수 있는 방안으로 생각된다.

[참 고 문 헌]

[1] 정보통신부, "Broadband IT Korea 건설을 위한 광대역 통합망 구축 추진 현황 및 계획", 2004. 9

[2] 전황수, 조원진, "미국의 차세대 네트워크 전략"

[3] 전자신문, "일본, u사회 구현 '시동'", 2004.6

[4] ITU, "Draft ITU-T Recommendation X.805, Security architecture for systems providing end-to-end communications"

[5] 손승원, "네트워크 보안 기술의 현재와 미래"

[6] 서동일, 김광식, 장종수, 손승원, "IT839 전략 추진을 위한 정보보호 기술개발 방향"

[7] 박진우, 김영부, 박경준, "IT839 기반기술 BcN의 배경과 발전"

[8] 양경윤, "웹 애플리케이션 보안 솔루션", 2005

[9] 이용균, "조기경보시스템 기술동향", 2005

[10] 최진기, "네트워크 인프라 보호 (3대 인프라의 안정성 확보)", 2004. 11

이명수

1989년 연세대학교 대학원 전자공학과 공학박사
1990년 ~ 1994년 KT 무궁화 위성사업 위성기술부장
1994년 ~ 1995년 KT 사업개발단 이동통신부장 (PCS 사업개발)
1996년 ~ 1999년 KT 무궁화 3호위성사업 추진 위성통개발팀장
1999년 ~ 2001년 KT 법인영업단 고객관리분야 팀장
2001년 ~ 2003년 KT e-Biz 본부 커머스/컨텐츠 사업팀장
2004년 ~ 현재 정보보호본부 정보보호기술담당, 한국정보보호학회 협동이사
관심분야 : 서비스 플래폼 사업개발, 네트워크 보안, 프라이버시 보호, 보안분야 서비스 및 사업개발

양재수

1981년 한국항공대학 통신공학과 (학사)
1985년 건국대학교 전자공학과 (석사)
1992년 미 뉴저지공과대학(NJIT) (공학박사)
1999년 서울대 MBA 과정 (수료)
현재 광운대학교 산학협력단 교수
관심분야 : BcN, 정보보호및보안, RFID 및 USN, 홈 네트워킹