X.805를 확장한 BcN 취약성 분류 체계

윤 종 림[†] · 송 영 호[††] · 민 병 준[†††] · 이 태 진[††††]

요 약

광대역통합망(BcN: Broadband Convergence Network)은 통신과 방송을 융합하여 유무선의 고품질 멀티미디어 서비스를 제공하기 위한 중요한 기반구조이다. 그러나 망의 융합에 따라 개별 망에서 발생한 침해 사고의 피해가 확산될 위험이 있고 수직 및 수평적 이동이 가능한 다양한 서비스가 출현함에 따라 새로운 위협 요인들이 발생하게 된다. 이에 효과적으로 대응하기 위해서는 BcN의 취약성을 시스템 구조적으로 분석하고 체계적으로 분류하여 이 결과가 공격 대응 기술을 마련하는데 활용되도록 해야 한다. 이를 위하여 본 논문에서는 보안 아키텍처 구성요소를 정의한 ITU-T의 X.805 권고안을 기반으로 BcN 환경에 적합하게 확장한 새로운 취약성 분류 체계를 제안한다. 이 새로운 분류는 서비스별로 보호해야 할 대상, 가능한 공격 수단, 그로 인한 피해 종류 및 위험도, 이를 막는데 효과적인 대응수단을 포함한다. 본 논문에서 제시하는 분류 체계를 기존의 CVE(Common Vulnerabilities and Exposures)와 CERT/CC(Computer Emergency Response Team/Coordination Center)의 취약성 정의 및 분류 방법과 비교하고, 체계 검증의 일환으로 BcN 서비스 중 하나인 VoIP(Voice over IP)에 적용한 사례와 취약성 데이터베이스 및 관리 소프트웨어 개발 결과에 대하여 논한다. 이 논문에서 제시한 연구 결과는 보안 지식을 집적하고 새로운 정보보호기술을 도출하는데 활용될 수 있다.

키워드 : 취약성, 광대역통합망, 보안 프레임워크

Classification of BcN Vulnerabilities Based on Extended X.805

Jong Lim Yoon[†] · Young Ho Song[††] · Byoung Joon Min[†††] · Tai Jin Lee[††††]

ABSTRACT

Broadband Convergence Network(BcN) is a critical infrastructure to provide wired-and-wireless high-quality multimedia services by converging communication and broadcasting systems. However, there exist possible danger to spread the damage of an intrusion incident within an individual network to the whole network due to the convergence and newly generated threats according to the advent of various services roaming vertically and horizontally. In order to cope with these new threats, we need to analyze the vulnerabilities of BcN in a system architecture aspect and classify them in a systematic way and to make the results to be utilized in preparing proper countermeasures. In this paper, we propose a new classification of vulnerabilities which has been extended from the ITU-T recommendation X.805, which defines the security related architectural elements. This new classification includes system elements to be protected for each service, possible attack strategies, resulting damage and its criticalness, and effective countermeasures. The new classification method is compared with the existing methods of CVE(Common Vulnerabilities and Exposures) and CERT/CC(Computer Emergency Response Team/Coordination Center), and the result of an application to one of typical services, VoIP(Voice over IP) and the development of vulnerability database and its management software tool are presented in the paper. The consequence of the research presented in the paper is expected to contribute to the integration of security knowledge and to the identification of newly required security techniques.

Key Words : Vulnerability, Broadband Convergence Network, Security Framework

1. 서 론

정보통신부가 추진하고 있는 IT839 전략에 있어서 가장 중요한 것은 모든 서비스와 신 성장 동력 산업의 기반이 되는 3대 기반구조의 성공적인 구축 여부이다. 그 가운데서도 통신 · 방송 · 인터넷을 통합하는 광대역통합망(BcN: Broadband Convergence Network)이 핵심 기반구조가 될 것이다.

BcN의 새로운 위협요소를 살펴보면, 기존에는 각각의 망들이 분리되어 있기 때문에 한 망에서 발생한 피해는 그 망의 범위를 벗어나지 못했지만, BcN에서는 모든 망들이 하나로 통합되고 융합됨으로 인해 개별 망에서 발생한 피해가 연결된 다른 모든 망으로 확산될 가능성이 매우 높다는 것이다. 둘째로 BcN은 최종적으로 IPv6를 기반으로 하기 때

※ 이 논문은 2005년도 인천대학교 자체연구비의 지원을 받았음.
본 연구는 한국정보보호진흥원 용역 결과를 반영한 것임.
† 정 회 원 : 나일소프트 소프트웨어연구소 선임연구원
†† 정 회 원 : 나일소프트 소프트웨어연구소 연구소장
††† 종신회원 : 인천대학교 컴퓨터공학과 교수
†††† 정 회 원 : 한국정보보호진흥원 주임연구원
논문접수 : 2005년 12월 6일, 심사완료 : 2006년 6월 1일

문에 IPv4 망에서 없었던 새로운 위협요소가 발생할 가능성이 높다. 또한 단기적으로는 IPv4 망과 IPv6 망이 혼재됨에 따른 취약성이 증가할 것이다. 셋째는 RFID/USN의 확산에 따른 서비스 거부 공격과 개인 사생활에 대한 위협요소가 증가하게 될 것이다[1].

다양한 보안 취약점을 이용한 악의적인 공격으로부터 네트워크 및 서비스를 안전하게 보호할 수 있는 보안기술을 개발할 필요가 있다. 또한 유효 사용자를 구별하고 다양한 정보기기 간에 안전한 통신 및 제어를 가능하게 하며, 다양한 침입으로부터 네트워크 자원을 보호할 수 있는 보안 기반구조 구축기술을 개발할 필요가 있다. BcN에서의 정보보호프레임워크를 도출하기 위한 방법론으로 X.805[2]를 사용함에 따라 BcN을 구성하는 각종 요소들을 보안 위협으로부터 보호하기 위한 정보보호요구사항이 도출되고, 이에 따라 요구사항을 만족시키기 위해 필요한 정보보호요소기술들을 도출하는 것이 가능해질 것이다.

BcN 정보보호프레임워크를 도출하는데 필요한 각각의 정보들은 서로 상관관계를 가짐으로 인해 체계적으로 관리해야 할 필요가 있다. 게다가 각 정보들을 연계하여 보다 조직적이고 체계적으로 정보보호프레임워크를 도출하기 위해서는 그 절차를 명확히 규정하고 자동화할 필요가 있다. 따라서 이 정보들을 데이터베이스화하고 이를 이용하여 정보보호프레임워크 도출 절차를 자동화하는 도구를 만들 필요성이 있는 것이다[3, 4]. 이렇게 함으로써 앞으로 새로이 늘어나게 될 여러 가지 서비스들과 BcN 구성요소들에 대한 정보보호프레임워크 도출에 효과적으로 대응할 수 있게 될 것이다. 또한 다양한 정보보호프레임워크 정보를 데이터베이스화하여 보유함으로써 BcN에 서비스/구성요소가 추가될 때 이에 대한 취약성 정보를 손쉽게 도출하여 이에 대한 보호대책을 적절히 강구하였는지 검증할 수 있게 될 것이다.

본 논문의 2장에서는 BcN의 취약성을 분석하고 체계적으로 분류하기 위한 관련 연구를 소개한다. 보안 아키텍처 구성요소를 정의한 ITU-T의 X.805 권고와 기존의 취약성 분류 방법들을 비교한다. 3장에서는 BcN 환경에 적합하게 확장한 새로운 취약성 분류 체계를 제안한다. 이 분류는 서비스별로 보호해야 할 대상, 가능한 공격 수단, 그로 인한 피해 종류 및 위험도, 이를 막는데 효과적인 대응수단을 포함한다. 이를 토대로 개발한 취약성 데이터베이스 및 관리 소프트웨어를 4장에서 설명하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

이 장에서는 우선 BcN 정보보호 문제를 살펴보고, BcN 취약성 분류의 기본 틀로 사용할 ITU-T의 X.805 권고안을 요약한다. 그리고 지금까지 발표된 대표적인 취약성 분류 방법들을 소개하고 비교한다.

2.1 BcN 보안 위협

한국전산원의 BcN 표준 모델에 의하면 BcN은 서비스 및 제어, 전달망, 가입자망, 홈네트워크 및 단말의 네 개 계층으로 나누어지고, 고품질 멀티미디어 서비스를 비롯한 음성·데이터, 유무선, 통신·방송 융합 서비스를 제공하는 것으로 되어 있다. 이와 같은 융합의 결과로 BcN은 기존의 네트워크와 달리 다음과 같은 새로운 보안 문제를 가지고 있다[1,5].

(1) 유무선 통신망과 방송망의 융합에 따라 개별망의 피해가 전체 네트워크의 피해로 확산될 우려
(2) 다양한 형태의 사업을 연계하는 개방형 인터페이스와 컨텐츠 및 솔루션 네트워크의 연동 과정에서의 취약성
(3) 이동성을 지원하는 복합 단말의 불안전성

지금까지 발표된 취약성 분석 결과를 보면, 서비스 및 제어 계층에서는 개방 인터페이스 접근 인증 및 권한의 오남용, 전송과 제어를 분리하는 소프트스위치 및 서버의 신뢰성 보장이 미비한 것으로 되어 있다. 전달망 계층에서는 IPv4와 IPv6의 변환 과정에서의 문제, 가입자망 계층에서는 서비스 자체를 무력화시킬 수 있는 DDoS(Distributed Denial of Service) 공격 취약성 등이 존재한다. 홈네트워크 및 단말 계층에서는 바이러스, 웜, 악성 스크립트, 해킹 및 위변조가 발생할 가능성이 높은 것으로 알려져 있다[5, 6].

2.2 ITU-T X.805 권고

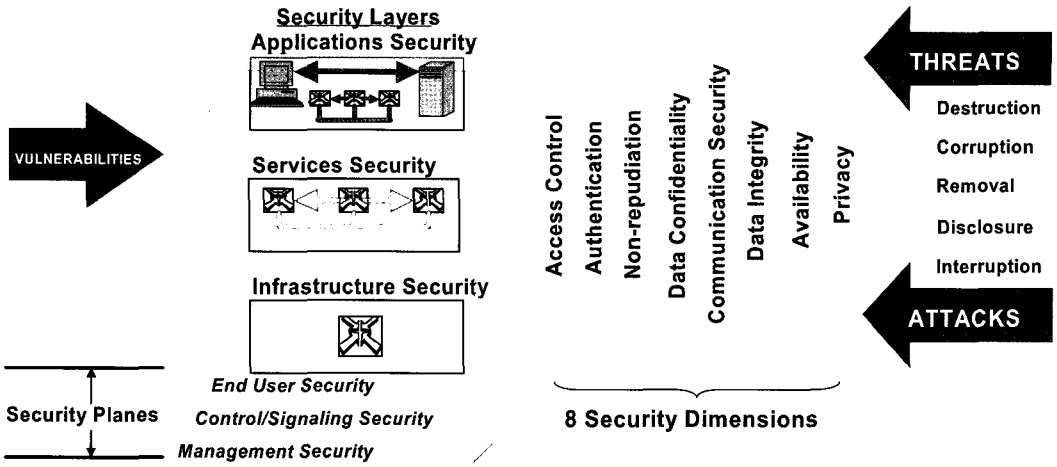
ITU-T의 X.805[2]는 단대단 네트워크 서비스의 보안 문제를 하향식으로 접근한 것으로, 보안의 취약성을 도출하고 제대로 대응하기 위한 목적으로 만들어졌다. 복잡한 네트워크의 보안 문제를 논리적인 구성요소들로 분리하는 접근방법을 취하고 있다.

네트워크 구성요소를 보안 계층과 보안 평면으로 나눈다. 보안 계층은 응용, 서비스, 기반구조의 세 계층으로, 평면은 단말 사용자, 제어 및 신호, 관리의 세 평면으로 나눈다. 따라서 보안 구성요소는 모두 아홉 개의 모듈로 이루어진다. 보안의 대응 기술을 접근제어, 인증, 부인봉쇄, 데이터 기밀성 유지, 통신보안, 데이터 무결성 보장, 가용성, 개인정보보호의 기술로 분류하고 있다. 보안의 위협은 정보나 자원의 파괴, 정보의 변조, 정보나 자원의 손괴, 정보 누설, 서비스 중단으로 정의한다. (그림 1)에 이 보안 아키텍처를 나타내었다.

X.805의 보안 아키텍처는 복잡한 네트워크의 보안 문제를 논리적인 구성요소들로 분리해서 조명하는 접근방법을 취하고 있기 때문에 BcN과 같은 복합 망에서의 보안 문제를 다루는데 유용하게 사용될 수 있다. 실제로 ITU에서 2006년도에 발표한 NGN(Next Generation Network) 관리 규격[7]을 보면 보안 관리에서 X.805를 이용하는 것으로 되어 있으며 [8]에서 X.805를 NGN 관리에 적용시킨 사례를 찾아 볼 수 있다.

2.3 기존 취약성 DB

CVE(Common Vulnerabilities and Exposures)[9,10]는 미국 국토안보부의 지원 아래 비영리 기관인 MITRE에 의해 운영되는 것으로서, 보안 취약점에 관한 간명한 기술과 함



(그림 1) ITU-T X.805 보안 아키텍처

께 보안 관련 여러 업체와 기관들에 의해 제각각 이름 붙여지고 조금씩 상이한 설명들을 표준화하는 것을 목적으로 한다. 따라서 CVE는 엄밀히 말하자면 데이터베이스가 아니라 개개의 취약성에 대한 정의를 붙여 놓은 일종의 사전에 불과하다. 다른 취약성 데이터베이스들에 포함되어 있는 상세한 설명, 위험도, 취약성 분류, 대응 방법 등의 정보가 포함되어 있지 않다.

CERT Coordination Center(CERT/CC)[11,12]는 카네기 멜런 대학교에 의해 1988년에 설립된 인터넷 보안 분야의 권위 있는 연구 기관이다. CERT/CC에서는 "Vulnerability Notes"라고 하는 취약점 데이터베이스를 운영하고 있었는데 9.11 테러 이후 국토안보부가 신설되면서 정부에 의해 운영되는 US-CERT로 데이터베이스 운영권이 이전되었다. 취약성 이름, 개요, 설명, 영향, 해결책, 임시조치, 발견자, 참조정보 등을 제공한다.

KCVE(Korea Common Vulnerabilities and Exposures)는 한국정보보호진흥원(KISA)에서 2003년 개발 완료한 취약성 데이터베이스이다. 현재 인터넷침해사고대응지원센터 홈페이지에서 KCVE 데이터베이스를 이용한 보안 취약점 검색 서비스를 일반에 제공하고 있다. KCVE가 제공하는 정보는 취약성 분류, 등급, 공지 일자, 관련 포트, 취약한 패키지, 영향, 공격 시나리오, 예방책, 해결방안, 참조 등 매우 다양하다.

위의 세 가지 취약성 데이터베이스는 모두 최신 정보를 잘 유지하고 있다. CVE가 취약점에 대한 간단한 정의 및 참조 연결만을 제공하는 반면에, CERT/CC는 상세한 설명과 함께, 영향, 조치 방안, 관련 제품 등 비교적 상세한 정보를 포함하고 있고 KCVE는 이러한 정보는 물론이고 공격 시나리오 정보와 원격 및 지역, 오류 범주 정보를 제공한다.

3. BcN 취약성 분류 방법

취약점은 분류하는 데에는 여러 가지 방법이 있을 수 있다. 취약점 데이터베이스를 구축 운영하고 있는 여러 기관의 분류 방식을 살펴보면 다음과 같은 것들이 있다.

(1) 오류 범주별 분류 (예, 변수 범위 오류, 사용자 검증 오류, 정보 출처 검증 오류, 입력 값 유효성 판단 오류, 예외사건 처리 오류, 경쟁 상태 발생 오류, 사건 직렬화 오류, 트랜잭션 오류, 환경 및 시스템 설정 오류 등)
(2) 공격 결과별 분류 (예, 접근 권한 획득, 보안 대책 우회, 파일 조작, 데이터 변조, 정보 획득, 서비스 거부 공격 발생, 주변 정보 획득 등)
(3) 위험도별 분류 (예, 결과의 치명도에 따라 3-5단계 구분)

이 장에서는 구조적으로 융합된 망에서 다양한 서비스를 제공하는 BcN의 특성에 따라 취약성을 분류하기 위한 항목과 세부 분류 기준을 제시한다.

3.1 BcN 서비스별 분류

BcN 구축을 위한 서비스 및 제어 계층의 단계별 목표는 음성·데이터 통합서비스와 유·무선 연동 및 통합서비스를 제공하는 제1단계부터 시작한다. 제2단계 목표는 본격적인 품질 보장 서비스, 가능한 멀티미디어 영상 통화 및 회의 통화 서비스, 통신·방송 융합서비스, 홈 네트워킹 서비스 등을 제공하는 것이다. 마지막으로 서비스 및 제어계층 제3단계에서는 1, 2단계 서비스는 물론 RFID/USN 서비스와 텔레매틱스 서비스까지 포함하는 진정한 의미의 BcN 융합서비스를 제공하는 것을 목표로 하고 있다[4]. 이로 미루어 볼 때 BcN 서비스는 새롭게 정의되어 추가될 수 있는 가능성이 매우 크다. 따라서 IT839에서 정의된 8대 서비스(2.3GHz 휴대인터넷, DMB, 홈네트워크, RFID, W-CDMA, 텔레매틱스, DTV, VoIP)와 3대 기반구조(BcN, IPv6, USN)를 근간으로 취약성을 분류하며 새로운 서비스 혹은 기반구조를 추가할 수 있도록 한다.

IT839의 8대 서비스 혹은 3대 기반구조에 대해 취약성을 분류하면 취약점, 정보보호요구사항을 체계적으로 파악할

수 있으므로 해당 서비스의 취약성을 일목요연하게 파악할 수 있고 정보보호요소기술의 신규 개발 필요성을 파악할 수 있는 근간이 된다.

3.2 보호대상별 분류

X.805 방법론에 기초한 취약성 분석 과정은 정보보호 계층/평면 분류를 근거로 보호대상을 식별하고 이를 대상으로 우선순위 평가를 진행하여 우선보호대상을 선정한다. 그리고 각 보호대상에 대해 취약성을 분석하게 된다. 따라서 보호대상에 따라 취약성을 분류할 필요가 있다.

보호대상은 8대 서비스 및 3대 기반구조를 구성하는 각 요소들을 포함하고 있다. 따라서 특별히 중요한 구성요소들에 대해서 어떤 취약성이 있는지 알 수 있고, 이에 따라 정보보호요구사항/요소기술을 적용하여 조기에 보호 대책을 강구할 수 있다. 또 이를 검증하기 위해 취약점 DB와 연계하여 보호 대책이 제대로 강구되었는지 검증할 수 있다.

3.3 공격수단별 분류

시스템의 설계, 구현 및 운용 상에 존재하는 결함을 악용하는 공격수단에는 다음과 같은 것들이 있다.

- 장치에 대한 물리적 파괴 및 훼손
- 장치 도용 및 위조
- 스니핑(sniffing)
- 스푸핑(spoofing)
- 재연(replaying)
- 트래픽 모니터링
- 보안 우회
- 세션 가로채기
- 강제 리셋
- 원격 코드 실행
- 패스워드 크래킹(password cracking)
- 버퍼 오버플로우
- 자원 고갈
- 백도어

이와 같은 수단 외에 다른 방법들을 추가할 수 있도록 고려한다.

3.4 대응방안별 분류

대응방안은 다음의 X.805의 8가지 대책을 적용한다.

(1) 접근제어 : 비인가자가 정보통신시스템에 부정한 방법으로 접근하여 사용하는 것을 방지
(2) 인증 : 정보의 송수신자 또는 정보시스템 이용자의 신원을 식별 및 확인
(3) 부인 봉쇄 : 사용자가 정보통신시스템을 통하여 정보를 송수신하거나 처리한 사실을 부인하는 것을 방지
(4) 데이터 기밀성 : 전송 또는 보관중인 정보를 비인가자가 부정한 방법으로 입수하더라도 그 내용을 알 수 없도록 보호
(5) 통신 보안 : 정보가 송신자로부터 수신자에게 정확하게 전달되도록 중간 경로를 보호
(6) 데이터 무결성 : 전송 또는 보관중인 정보를 인가되지 않은 방법으로 위조 또는 변조할 수 없도록 보호
(7) 가용성 : 네트워크 요소, 서비스, 응용을 적법한 사용자들이 이용할 수 있도록 보장
(8) 개인정보 : 개인정보의 유출 차단

3.5 공격결과별 분류

X.805 방법론을 이용하여 분류한다. X.805에 제시된 위협 모델에 의한 공격 결과는 아래와 같이 5가지가 있다.

(1) 파괴 : 정보나 네트워크 자원의 파괴
(2) 변조 : 비인가자에 의한 자원의 변조
(3) 도용 : 정보나 자원 절도
(4) 유출 : 비인가자에 의한 자원 접근
(5) 중단 : 네트워크 자원 접근 방해

위협에 따라 취약성을 분류하여 공격결과의 종류별로 취약성의 경중을 알아낼 수 있고, 이로써 대응해야 할 위협의 우선순위를 정할 수 있다.

3.6 위험도별 분류

모든 취약성은 어떤 대상에 대한 것인지, 어떤 영향을 미칠 것인지, 복구가 얼마나 어려울 것인지 등 파급효과가 모두 다르다. 따라서 취약성을 파급효과 또는 위험도별로 분류할 필요가 있어 다음과 같이 세 단계로 분류한다.

(1) 고 : BcN 전체 또는 상당히 큰 규모의 망이 작동하지 못하거나, 서비스/구성요소 대부분이 정상 작동하지 못하는 등 파급효과가 큰 취약성
(2) 중 : 국지적인 망이 작동하지 못하거나 특정 BcN 서비스/구성요소가 작동하지 못하는 등의 파급효과를 발생시키는 취약성
(3) 저 : 보호되어야 할 서비스/구성요소에 관한 정보가 유출되거나, 영향력이 적은 특정 장비가 오작동하는 등의 파급효과를 발생시키는 취약성

취약성에 대한 위험도 부여의 객관성이 다소 어려운 작업이지만 특정 서비스 혹은 기반구조에 대한 위험도를 정량적으로 평가할 수 있는 기초 데이터가 될 수 있다. 또한 새로운 서비스나 기반구조가 추가될 때 사전에 취약성 평가를 하여 대응의 우선순위를 결정할 수 있다.

<표 1>은 이상에서 정의한 취약성 분류 항목을 요약한 것이다. 이 분류 체계를 BcN의 서비스 중 하나인 VoIP에 적용한 결과를 <표 2>에 나타내었다.

이상에서 제안한 분류체계를 기존의 분류 방법과 비교하면 <표 3>과 같다. 이 결과로 볼 때, 본 논문에서 제안하는 분류 체계는 기존의 방법 보다 구체적이고 특히, 분류 구성요소들 간의 연관성을 제공하여 전체적인 보안 프레임워크를 마련하는데 매우 중요한 구실을 한다.

〈표 1〉 취약성 분류 항목

분류항목	분류 내역	비고
서비스	2.3GHz 휴대인터넷, 위성/지상파 DMB, 홈네트워크, RFID, W-CDMA, 텔레매틱스, 지상파 DTV, 인터넷전화 (VoIP)	8대 서비스
계층(Layer)	기반구조(Infrastructure), 서비스, 응용 보안 계층	계층
평면(Plane)	사용자, 제어/신호, 관리 보안 평면	행위
공격수단	버퍼 오버플로우, 조작된 패킷/메시지, 무선신호특성 등	
정보보호요구사항 (Dimension)	접근 제어, 인증, 부인 봉쇄, 데이터 기밀성, 통신 흐름 보안, 데이터 무결성, 가용성, 프라이버시	대응 기술
공격결과 (Threat)	파괴(Destruction), 변조(Corruption), 도용(Removal), 유출(Disclosure), 중단(Interruption)	피해유형, 공격결과
위험도 (Risk)	고, 중, 저	위험도, 파급효과
구성요소	라우터, 홈네트워크 단말, 서버, 방화벽 등	보호대상

〈표 2〉 분류 체계의 VoIP 적용 사례

Layer/ Plane	보호대상	취약성	공격수단	공격결과	공격결과설명	위험도	정보보호 요구사항	정보보호 요구사항 설명	정보보호 소요기술
기반계층 관리행위	로컬 및 원격 관리 정보	텔넷의 인증 취약성	엿듣기 속이기	정보의 노출 텔넷 접속	서버에 대한 스니핑 및 스푸핑을 통해서 관리 정보를 획득	Med	통신 보안 접근 제어	텔넷의 인증에 대한 인증과 관리정보를 암호화함	인증 프로토콜 IPSec, TLS
	HTTP, Telnet, FTP	서버에 대한 DoS 취약성	자원고갈	서비스 중단	서버에 대한 DoS 공격으로 인해 자원 고갈 및 서비스 중단	Low	가용성	서버는 침입을 탐지하고 대응해야 함	침입탐지 시스템 침입차단 시스템 침입 방지 시스템
기반계층 제어행위	라우팅 테이블, ARP 테이블, ATM 및 MPLS 링크제어 정보	테이블 정보나 링크제어 정보에 대한 스니핑 취약성	엿듣기 속이기	정보의 노출 정보의 변조	라우팅 테이블, ARP 테이블 등 관리 정보를 스니핑하거나 위조하여 관리 정보 획득	Low	기밀성 통신 보안	데이터 암호화	IPSec, TLS
기반계층 사용자행위	사용자 정보	ID, 패스워드 추측	위장	정보의 노출 정보의 변조	IP Phone 단말의 사용자 ID 및 패스워드 추측	Med	인증	사용자 인증	소유를 기반 인증 생체 기반 인증
		패스워드 노출	위장	정보의 노출 정보의 변조	IP Phone 단말의 사용자 패스워드 추측	Med	인증	사용자 인증	소유□ 기반 인증 생체 기반 인증
		IP 주소 정보 획득	엿듣기	정보의 노출 정보의 변조	IP Phone에 연결된 허브를 통해 IP주소 스니핑	Low	기밀성	데이터 암호화	IPSec, TLS
서비스계층 관리행위	TFTP	TFTP 서버 삽입 공격 취약성	속이기	정보의 노출 정보의 변조	IP Phone이 리셋 될 때, DHCP response를 위조하여 IP Phone의 설정 변경	Low	무결성 인증	데이터 암호화	IPSec, TLS
	DHCP	DHCP 서버 삽입 공격 취약성	취약점 악용 중간자 공격	정보의 노출 정보의 변조	IP Phone이 부팅할 때, DHCP response 정보를 악의적으로 변조하여 설정을 불법적으로 변경	Low	무결성 인증	데이터 암호화	IPSec, TLS
서비스계층 제어행위	SIP, H.323, MGCP, MEGACO/H.248, SIP-T, SCTP	SIP 프로토콜 스택에서의 버퍼 오버플로우 취약성	버퍼 오버플로우	서비스 중단 정보의 노출	SIP 프로토콜 스택에 버퍼오버플로우 취약성을 이용해 서비스를 침해	Low	가용성 통신 보안	버퍼오버플로우에 대해서 탐지 및 대응을 하고 데이터를 암호화함	침입탐지 시스템 침입차단 시스템 침입 방지 시스템 IPSec, TLS
		H.323 프로토콜 스택에서의 DoS 공격 취약성	자원 고갈	서비스 중단	H.323 프로토콜 스택에 임의 코드주입으로 인한 DoS공격 가능	Low	가용성	서버는 침입을 탐지하고 대응해야 함	침입탐지 시스템 침입차단 시스템 침입 방지 시스템
서비스계층 사용자행위	SIP, H.323, SMTP, HTTP	트래픽 도청 취약성	엿듣기	정보의 노출	VoIP 제어 정보를 중간에서 도청 가능	Med	데이터 기밀성 통신 보안	데이터 암호화	해쉬 함수 국내표준: HAS-160 IPSec, TLS
응용계층 관리행위	VoIP 단말 및 응용프로그램	디폴트 패스워드 취약성	엿듣기	정보의 노출 정보의 변조	IP Phone에 설정된 디폴트 패스워드를 통해 정보 획득	Med	기밀성 인증	사용자 인증	소유를 기반 인증 생체 기반 인증
		소프트웨어 취약성	버퍼오버플로우 취약점 악용	정보의 노출 정보의 변조	버퍼오버플로우나 부적절한 패킷 헤더 처리로 인한 소프트웨어의 취약성을 통해 정보 획득	Med	데이터 기밀성	취약성 제거	취약성 진단 도구
응용계층 제어행위	VoIP 단말 및 응용프로그램	IP Phone의 웹서버에 대한 DoS 공격 취약성	서비스 중단	서비스 중단	IP Phone의 웹서버에 대한 파라미터 조작으로 DoS공격 가능	Low	가용성	침입을 탐지하고 대응함	침입탐지 시스템 침입차단 시스템 침입 방지 시스템
응용계층 사용자행위	단말 및 데이터 정보	스니퍼를 이용한 패킷 캡처 취약성	엿듣기	정보의 노출	스니핑을 통해서 얻은 정보를 이용해 접근권한이나 정보를 수집	Med	인증 접근 제어	사용자 인증	유/무선 PKI 장치 인증
	사용자의 식별정보와 그 행위	VoIP 단말의 비인가 장치에 대한 취약성	위장	불법 접속	사용자와 사용장치의 행위에부터 위장	Med	부인 봉쇄	행위자 및 장치의 식별	로그 기록, 전자서명
	음성정보, 음성메일	VoIP 스팸 및 음성 메일 폭탄 취약성	스팸 공격	서비스 중단	VoIP 스팸 방생기를 사용해 서비스 가용성을 훔침	Low	가용성	스팸메일 대응	스팸 탐지 및 제거

〈표 3〉 기존의 분류 방법과의 비교

	CVE	CERT/CC	제안 분류 체계
목적	표준화된 취약점 설명	취약점 대응	취약점 분석 및 대응에 필요한 기술 도출
형태	취약점 기술 사전	취약점 데이터베이스	취약점 데이터베이스
분류기준	일련번호	이름, 개요, 설명, 영향, 해결책, 임시조치, 발견자, 참조정보	각 계층 및 평면 별 보호대상, 취약성, 공격수단, 공격결과,위험도, 정보보호요구사항, 정보보호에 필요한 기술
활용	다양한 기관에서 발견된 취약점을 공통으로 인지하고 대응	취약점을 데이터베이스화해서 효과적으로 대응할 수 있도록 지원	분류구성요소간의 연관성을 제공하여 효율적 보안 프레임워크 구축 지원

4. 취약성 DB 및 관리 소프트웨어

이 장에서는 3장의 분류 체계를 바탕으로 개발한 취약성 DB와 관리 소프트웨어에 대하여 설명한다.

4.1 취약성 DB 스키마 설계

취약성 DB에 입력해야 할 정보 요소들을 나열해 보면 다음과 같다.

취약성 ID, 취약성 , 취약성 설명, 참조 정보, 서비스/기반구조 ID, 서비스/기반구조 이름, 서비스/기반구조 설명, 위협 ID, 공격결과 이름, 공격결과 설명, 공격수단 ID, 공격수단 이름, 공격수단 설명, 모듈(Plane/Layer) ID, 모듈 설명, 보호대상 ID, 보호대상 이름, 보호대상 설명, Dimension ID, Dimension 이름, Dimension 설명, 위험도 ID, 위험도, 위험도 설명, 사용자 ID, 사용자 이름, 사용자 직책, 사용자 직급, 소속 부서, 사용자 권한, 사용자 패스워드, 작업일시, 작업구분, 변경 전, 변경 후, 작업 ID, 작업 이름, 작업 설명 등이다.

식별된 정보들을 정규화를 거쳐 객체로 분류하고 기본 키로 사용될 수 있는 정보와 각 키와 연관된 속성을 다음과 같이 정의한다.

(1) 취약성(Vulnerability) 객체

취약성 DB에 저장될 여러 가지 정보들 가운데 핵심이 되는 기본 객체이다.

- 취약성 ID(vul_id) : 취약성에 대한 식별자(기본키)
- 취약성 이름(name) : 취약성에 대한 이름
- 취약성 설명(description) : 취약성에 대한 설명
- 참조링크(reference) : 취약성에 대한 참조 정보

(2) 서비스인프라(ServiceInfra) 객체

8대 서비스 및 3대 인프라 객체이다. 이것은 향후 새로운 서비스 및 인프라로 확장될 가능성이 있음을 고려한다.

- 서비스인프라 ID(svcinfra_id) : 서비스인프라에 대한 식별자(기본키)
- 서비스인프라 이름(name) : 서비스/인프라 이름
- 서비스인프라 설명(description) : 서비스/인프라에 대한 설명

(3) 모듈(Module) 객체

취약성을 X.805 Plane/Layer에 따라 분류하기 위한 객체이다.

- 모듈 ID(module_id) : 모듈에 대한 식별자(기본 키)
- 모듈 이름(module_name) : 각 모듈의 이름
- 모듈 설명(module_description) : 각 모듈에 대한 설명
- Plane(plane) : X.805 3가지 Security Plane
- Layer(layer) : X.805 3가지 Security Layer

(4) 공격수단(Exploit) 객체

위협요소들을 분류하기 위한 객체이다.

- 공격수단 ID(exploit_id) : 공격수단에 대한 식별자(기본 키)
- 공격수단 이름(exploit_name) : 각 공격수단의 이름
- 공격수단 설명(exploit_description) : 각 공격수단에 대한 설명

(5) 공격결과(Threat) 객체

취약성 분류 체계에서 사용될 공격결과 요소를 표현하는 객체이다.

- 공격결과 ID(threat_id) : 공격결과에 대한 식별자(기본키)
- 공격결과 이름(name) : 공격결과에 대한 이름
- 설명(description) : 범주에 대한 설명

(6) 보호대상(Target) 객체

취약성 분류 체계에서 사용될 보호 대상에 관한 객체이다.

- 보호대상 ID(tgt_id) : 보호 대상에 대한 식별자(기본키)
- 보호대상명(name) : 보호 대상 이름
- 설명(description) : 보호 대상에 대한 설명

(7) 정보보호요구사항(Dimension) 객체

취약성 분류 체계에서 사용될 정보보호요구사항에 관한 객체이다.

- 정보보호요구사항 ID(dim_id) : 정보보호요구사항에 대한 식별자(기본키)
- 정보보호요구사항 이름(name) : 정보보호요구사항 이름
- 설명(description) : 정보보호요구사항에 대한 설명

(8) 위험도(Risk) 객체

취약성 분류 체계에서 사용될 위험도(파급효과)를 표현하는 객체이다.

- 위험도 ID(risk_id) : 위험도에 대한 식별자(기본키)
- 등급(level) : 위험 등급
- 설명(description) : 위험도에 대한 설명

(9) 사용자(Users) 객체

취약성 DB에 접근할 수 있는 사용자들에 관한 객체이다.

- 사용자 ID(user_id) : 사용자에 대한 식별자(기본키)
- 사용자명(name) : 사용자 이름
- 직책(position) : 사용자 직위
- 직급(level) : 사용자 직급
- 부서(department) : 사용자 부서명
- 권한(authority) : 사용 권한
- 패스워드 : DB에 접근할 때 정당한 사용자인지 인증하기 위한 암호

(10) 작업유형(Work) 객체

사용자가 취약성 DB에 취약성 정보를 최초 입력, 수정, 삭제 등 수행한 작업에 대한 유형 분류 객체이다.

- 작업유형 ID(work_id) : 작업유형에 대한 식별자(기본키)
- 작업유형 이름(work_name) : 각 작업유형의 이름

• 작업유형 설명(work_description) : 각 작업유형에 대한 설명

(11) 변경이력(History) 객체

사용자가 취약성 DB에 접근, 입력, 수정, 삭제한 이력에 관한 객체이다.

• 취약성 ID : 취약성 객체를 참조하는 외래 키(복합기본키)
• 사용자 ID : 사용자 객체를 참조하는 외래 키(복합기본키)
• 작업일시(date) : 각 작업별 완료 일시
• 작업구분(work_id) : 작업의 종류(외래 키)
• 변경내역(history) : 사용자에 의해 이루어진 작업 내역

(그림 2)는 이상의 스키마 설계 내역을 다이어그램으로 표현한 것이다.

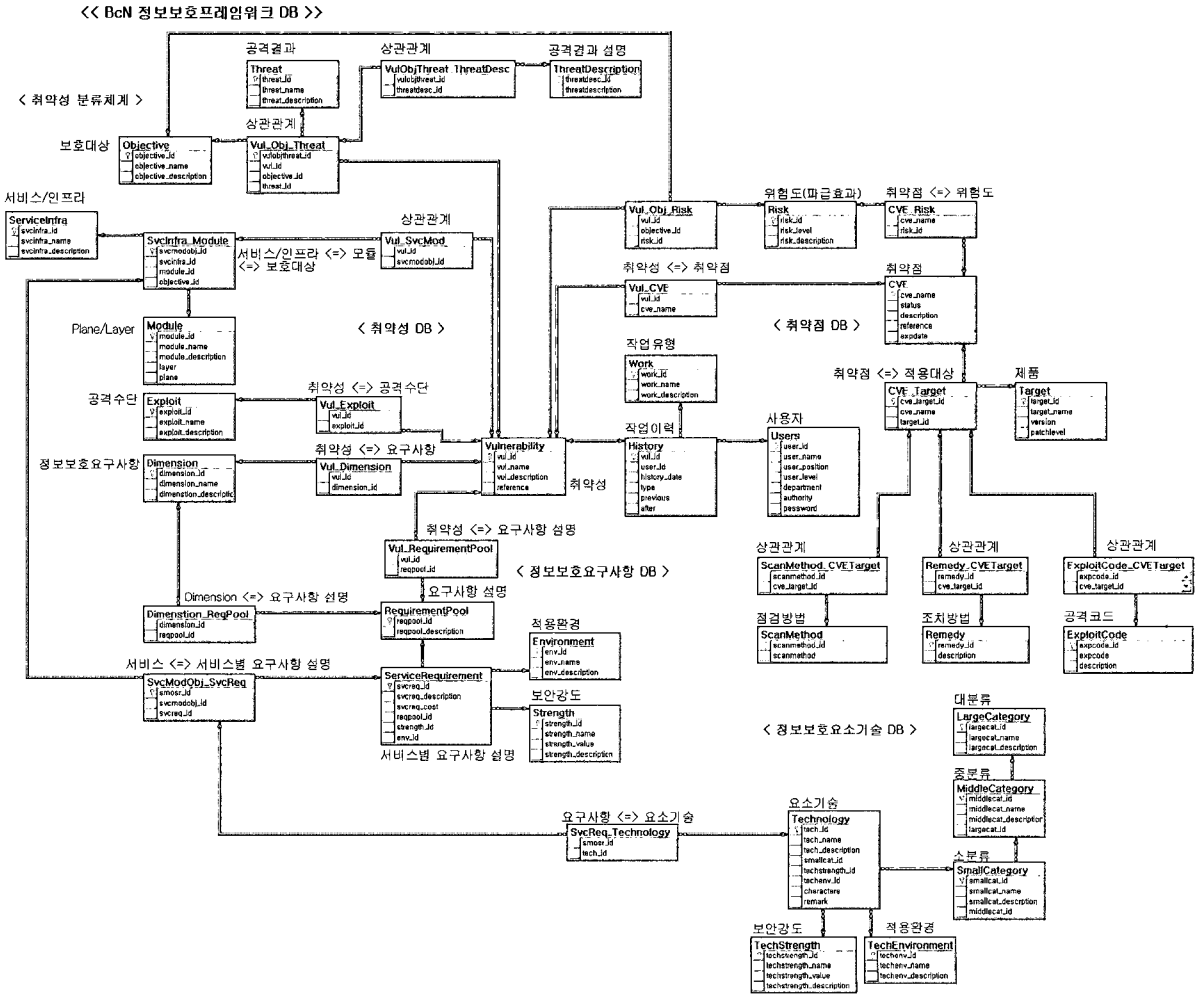
4.2 관리 소프트웨어 개발

BcN 정보보호프레임워크 DB에는 개념적으로 볼 때 크게 다음과 같은 네 가지 정보가 입력, 관리된다. 첫째, 취약성 정보로서 IT839 8대 서비스 및 3대 기반구조에 대한 취약성 분석 결과 도출되는 정보들이다. 둘째, 8대 서비스 및 3대 기반구조에서 발견, 공개되는 취약점 정보들이 포함된다. 셋째, 도출된 취약성을 보호하기 위해 요구되는 정보보호요구사항 정보가 포함된다. 넷째, 정보보호요구사항을 만족시키기 위해 필요한 정보보호 기술들이 포함된다.

이러한 네 가지 주요 정보들을 효과적으로 조직화함으로써 체계적으로 정보보호프레임워크를 도출하고 상관관계를 잘 정의하여 표현함으로써 의미 있는 결과를 도출할 수 있도록 지원하는 DB 관리 소프트웨어가 개발되었다. 이는 구현된 DB에 필요한 자료를 입력, 수정하고 정보보호프레임워크 도출을 위한 도구로 사용할 수 있는 관리 소프트웨어이다.

5. 결 론

차세대 IT 산업의 핵심 기반이 될 광대역통합망의 중요성과 보안 환경의 변화를 살펴보았고, 이에 효과적으로 대응하기 위해 BcN의 취약성을 분석하고 체계적으로 분류하기



(그림 2) 취약성 DB 스키마 설계

위한 체계를 제안하였다. 또한, 광대역통합망에 대한 분석과 취약성 분석을 통해 도출된 취약성 정보들을 체계적으로 관리할 수 있도록 데이터베이스를 설계하였다. 이 데이터베이스는 단순히 취약성만을 저장하는 것이 아니라 이를 검증하기 위하여 구체적 취약성 사례 데이터베이스와 연동하도록 설계하였다. 이로써 특정 서비스나 기반구조에 대한 취약성을 도출하고 그에 연관된 사례들을 도출하여 직접 분석을 함으로써 실제로 취약성이 존재하는지 검증할 수 있게 되었다. 또한 이 데이터베이스를 이용하여 실제 운영중인 서비스/기반구조에 대한 보안성 평가를 할 수 있게 되었다.

한편 이 데이터베이스에는 취약성을 보호/제거하기 위해 필요한 정보보호요구사항 및 정보보호요소기술 데이터베이스가 포함됨으로써, 새로이 구축될 서비스/기반구조에 대해서 정보보호프레임워크 도출 절차에 따라 사전에 취약성을 예측하고 설계 및 구축 단계에서부터 체계적으로 보안 대책을 강구해 나갈 수 있는 발판을 마련할 수 있게 되었다.

이 논문에서 제시한 연구 결과는 보안 지식을 집적하고 새로운 정보보호기술을 도출하는데 중요한 역할을 할 것으로 기대된다.

참 고 문 헌

[1] 정보통신부(한국전산원), "광대역통합망 기반구축사업에 관한 연구 (최종 연구개발 결과보고서)", 정보통신부, 2004년 12월.

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

[3] 한국정보보호진흥원, "정보보호표준화 로드맵", 2004.

[4] 한국정보통신기술협회, "IT839 전략 표준화 로드맵 종합보고서2", 한국정보통신기술협회, 2004년 12월.

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

[6] 김정태 외 3인, "유비쿼터스 홈서버 보안 요구사항 및 구현방안", 전자통신동향분석 제20권 제2호, 2005년 4월.

[7] ITU, "NGN Management Specifications," NGN Management Specification Roadmap, https://datatracker.ietf.org/documents/LIAISON, ITU Mangaement Work Group, 2006.

[8] Zachary Zeltsan, "ITU-T Recommendation X.805 and its Application to NGN," ITU Workshop on NGN in collaboration with IETF, Geneva, May, 2005.

[9] MITRE, "Common Vulnerabilities Exposures: The Key to Information Sharing," http://cve.mitre.org/docs/, 2005.

[10] Robert Martin, "Managing Vulnerabilities in Networked Systems," IEEE Computer Society Computer Magazine, Nov., 2001.

[11] CERT, CERT Advisory ca-2000-01: "Denial-of-service developments," http://www.cert.org/advisories/ca-2000-01.html, 2000.

[12] J.D. Howard, "An analysis of security incidents on the internet 1989-1995," http://www.cert.org/research, 2000.

윤 종 림

e-mail : abc@nilesoft.co.kr

1995년 육군사관학교 전산학과(학사)

2001년 윈포넷 주임연구원

2002년~현재 나일소프트 소프트웨어연구소 선임연구원

관심분야 : 시스템보안, 네트워크보안, 보안 취약점

송 영 호

e-mail : yhsong@nilesoft.co.kr

1984년 한양대학교 산업공학과(학사)

1998년 연세대학교 전자계산학과(석사)

1984년~1994년 LG전자 컴퓨터사업부 과장/선임연구원

1998년~2000년 혜전대학 전산과 겸임교수

1994년~현재 나일소프트 소프트웨어연구소 연구소장

관심분야: 시스템보안, 위험관리, 컴퓨터포렌식

민 병 준

e-mail : bjmin@incheon.ac.kr

1983년 연세대학교 전자공학과(학사)

1985년 연세대학교 전자공학과(석사)

1991년 미국캘리포니아대학교(UC어바인) 전기및컴퓨터공학과(박사)

1984년~1986년 삼성전자 연구원

1992년~1994년 KT 선임연구원

1995년~현재 인천대학교 컴퓨터공학과 교수

관심분야: 보안, 유비쿼터스 컴퓨팅

이 태 진

e-mail : tjlee@kisa.or.kr

2003년 포항공과대학교 컴퓨터공학과(학사)

2003년~현재 한국정보보호진흥원 주임연구원

관심분야 : 정보보호, 무선보안, 무선통신