X.805를 확장한 BcN 취약성 분류 체계

윤 종림**, 송영호***, 민병준***, 이태진****

요 약

광대역통합망(BcN: Broadband Convergence Network)은 동방과 송음을 통합하여 유무선의 고용량 멀티미디어 서비스를 제공하기 위한 중요한 기반구조이다. 그러나 방송에 따라 개방 송방에 따라 발생한 환경 사고의 피해가 확산될 위험이 있고 수익 및 수익성 이론 가정한 다양한 서비스가 출현함에 따라 새로운 위협 요인들이 발생하게 된다. 이에 효과적으로 대응하기 위해서는 BcN의 취약성을 시스템 구조적으로 분석하고 제계적으로 분류하여 이 결합과 공격 대응 기술을 마련하는데 활용할 수 있도록 해야 한다. 이에 본 논문에서는 보안 기반적 구성요소를 정의한 ITU-T의 X.805 통합용 기반으로 BcN 환경에 적합하게 확장한 새로운 취약성 분류 체계를 제안한다. 이 새로운 분류는 서비스 별로 보호해야 할 대상, 가능한 공격 수단, 그로 인한 피해 종류 및 위험도를 나타내는 효과적인 대응수단을 포함한다. 본 논문에서 제시하는 분류 체계는 기존의 CVV(Common Vulnerabilities and Exposures)와 CERT/CC(Computer Emergency Response Team/Coordination Center)의 취약성 경 및 분류 방법을 비교하고, 제계 공통의 입으로 BcN 서비스 중 하나인 VoIP(Voice over IP)에 적용한 사례와 취약성 메트릭스 및 관리 소프트웨어 개발 결과에 대하여 논한다. 이 논문에서 제시한 연구 결과는 보안 지식을 집합하고 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 Jiee****

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. 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 ITP30 전략에 있어서 가장 중요한 것은 모든 서비스와 신 상호 등록 사업의 기반이 되는 3대 기반구조의 성공적인 구축 여부이다. 그 가운데서도 통신·방송·인터넷을 통합하는 광대역통합망(BcN: Broadband Convergence Network)이 적혈 기반구조가 될 것이다.

BcN의 새로운 위협요소를 살펴보면, 기존에는 각각의 망들이 분리되어 있기 때문에 한 망에서 발생한 피해는 그 망의 영역을 벗어나지 못했지만, BcN에서는 모든 망들이 하나로 통합되고 활용됨에 따라 개별 망에서 발생한 피해가 연결된 다른 모든 망으로 확산될 가능성이 매우 높다는 것이다. 때문에 BcN은 최종적으로 IPv6를 기반으로 하기 때
문에 IPv4 망에서 없었던 새로운 위험요소가 발생할 가능성이 높다. 또한 단기간으로는 IPv4 망과 IPv6 망이 혼합될 때, 다양한 취약성이 증가할 것이다. 특히, RFID/USN의 확산에 따른 서비스 간의 공격과 개인 사생활에 대한 위험요소가 증가하게 될 것이다(1).

다양한 보안 취약점을 이용한 악의적인 공격으로부터 네트워크 및 서비스를 안전하게 보호할 수 있는 보안기술을 개발할 필요가 있다. 또한 유호 사용자를 구별하고 다양한 정책기 간에 안전한 통신 및 제어를 가능하게 하며, 다양한 참여자로부터 네트워크 자원을 보호할 수 있는 보안 기반조 구축기술을 개발할 필요가 있다. 블렌드의 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 정보보호기술을 도출하는 것이 가능할 것이다.

BcN 정보보호프레임워크를 도출하는데 필요한 각각의 정보요소들은 서로 상관관계를 가짐으로 인해 체계적으로 관리해야 할 필요가 있다. 게다가 각 정보요소들을 연계하여 보다 조작하기 위해서 정보보호프레임워크를 도출하기 위해 사가 그 절차를 명확히 규정하고 자동화할 필요가 있다. 따라서 이 정보요소들을 데이터베이스화하고 이를 이용하여 정보보호프레임워크 도출 절차를 자동화하는 도구를 만들 필요성이 있는 것이다(3, 4). 이렇게 함으로써 앞으로 새로운 높아지게 될 여러 가지 서비스들이 BcN 구성요소들에 대한 정보보호프레임워크 도출에 효과적으로 대응할 수 있게 될 것이다. 또한 다양한 정보보호프레임워크 정보를 데이터베이스화하여 보유함에 따라 BcN에서 서비스/구성요소가 추가될 때 이에 대한 취약성 정보를 손쉽게 도출하여 이에 대한 보호대책을 적절히 정구할 수 있게 될 것이다.

본 논문의 2장에서는 BcN의 취약성을 분석하고 체계화로 분류하기 위한 관련 연구를 소개한다. 보안 아키텍처 구성요소의 정의를 위한 ITU-T의 X.805 권고문과 기존의 취약성 분류 방법들을 비교한다. 3장에서는 BcN 취약성에 적합하게 정의한 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 개발된 취약성 데이터베이스 및 관리 소프트웨어 적용 장에서 설명하고, 마지막으로 5장에서 결론을 냈다.

2. 관련 연구

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

2.1 BcN 보안 위협

한국전산협의 BcN 표준 모델의 의하면 BcN은 서비스 및 제어, 전달망, 가입자, 홈네트워크 및 센터의 네 개 계층으로 나누어지고, 홍보될 범위마다 서비스의 범위가 열려있어 이러한 계층의 결과로 BcN은 기존의 네트워크와 달리 다음과 같은 새로운 보안 문제를 가지고 있다(1, 2).

(1) 유호성 통신망과 방송망의 통신에 따라 계층별의 피해가 전체 네트워크의 피해로 확산될 우려
(2) 다양한 형태의 서비스를 연결하는 계층별 인터페이스와 컨트롤 및 솔루션 네트워크의 연관 과정에서의 취약점
(3) 이동성을 지원하는 복합 단말의 불안정성

지금까지 발표된 취약성 분석 결과를 보면, 서비스 및 계층 계층에서는 가장 인터페이스 접근 인증 및 권한해달 등, 간섭 및 제어를 분리하는 소프트웨어적 및 서비스의 선형적 보안이 미흡한 것으로 되어 있다. 전달망 계층에서는 IPv4와 IPv6의 변환 과정에서의 문제, 가입망 계층에서는 서비스 자료를 무력화할 수 있는-DDoS(Distributed Denial of Service) 공격 취약점 등이 존재한다. 홈네트워크 및 단말 계층에서는 브라우저, 웹, 앱, 소프트웨어, 해킹 및 위변조가 발생할 가능성이 높은 것으로 알려져 있다(5, 6).

2.2 ITU-T X.805 권고

ITU-T의 X.805(2)는 단단한 네트워크 서비스의 보안 문제를 풀어가기 위한 것으로, 보안의 취약성을 도출하고 대응하기 위한 목적을 만들어졌다. 복잡한 네트워크의 보안 문제를 논리적인 구성요소로 분리하는 접근방법을 풀어가고 있다.

네트워크 구성요소를 보안 계층과 보안 레벨로 나누어 보안 계층은 응용, 서비스, 기반구조로 세 계층으로, 명령은 단말 사용자, 제어 및 신호, 관리의 세 레벨로 나누어 다. 따라서 보안 구성요소는 모두 이하 개의 모듈로 이루어진다. 보안의 대응 기술을 접근제어, 인증, 보안체크, 데이터 기밀성 유지, 보안성, 데이터 무단이용 방지, 가용성, 개인정보보호의 기술로 분류하고 있다. 보안의 결함은 보안의 점, 정보의 변경, 정보의 손실, 정보 누출, 서비스 중단으로 정의한다. (그림 1) 이 보안 아키텍처를 나타낸다.


2.3 기존 취약성 DB

CVE(Common Vulnerabilities and Exposures)[9,10]는 미국 국토안보부의 지원 아래 비영리 기관인 MITRE에 의해 운영되는 것으로, 보안 취약점에 관한 간행된 기술과 합
X.805을 확장한 BcN 취약성 분류 체계 249

위 보안 관련 여러 업계와 기관들에 의해 계발된 기존 분류를 바탕으로 하여, 이 기존 분류를 확장하고 개선한 새로운 분류체계를 제시한 바 있다. 

CERT Coordination Center(CERT/CC)는 최초로 취약성 분류를 정립한 기관으로 1988년에 설립된 인터넷 보안 분야의 전문 연구여당이다. CERT/CC는 "Vulnerability Notes"라고 하는 취약성 내용을 제공하고 있는데, 이를 기반으로 BcN 취약성 분류체계를 제시한다. 

KCVE(Korea Common Vulnerabilities and Exposures)는 한국정보보호진흥원(KISA)에서 2003년 개발, 발간한 취약성 데이터베이스이다. 현재 인터넷비해색고응용자원센터 홈페이지에서 KCVE 데이터베이스를 이용한 보안 취약점 검색 서비스를 일반에 제공하고 있다. KCVE는 취약성 정보를 제공하고 있는데, KCVE는 그전에 비해 보안 취약점 검색 서비스를 좀 더 자세히 제공하고 있다. 

위의 세 가지 취약성 데이터베이스는 모두 취약성 정보를 제공하고 있다. CVE가 취약점 데이터베이스를 제공한 다음에, CERT/CC는 경제, 경영, 인프라 구축, 관리 제공 등 비교적 상세한 정보를 제공하고 있으며, KCVE는 전체 정보를 제공하고 있다. 

3. BcN 취약성 분류 방법

취약점은 분류하는 데에는 여러 가지 방법들이 있을 수 있다. 

(1) 오류 범주별 분류 (예, 변수 범위 오류, 사용자 검증 오류, 정보 출처 검증 오류, 입력 없이 유 효성 판단 오류, 예외사항 처리 오류, 특정 상태 발생 오류, 사전 설정값 오류, 트래픽 오류, 하드웨어 설정 오류 등) 
(2) 공격 결과별 분류 (예, 접근 권한 획득, 보안 대책 우회, 파일 조작, 데이터 변조, 정보 획득, 서비스 기부 공격 발생, 주변 정보 획득 등) 
(3) 위협도별 분류 (예, 결과의 영향도에 따라 3-5단계 구분) 

이 방법들은 구조적으로 유망한 방향에서 다양한 서비스를 제공하는 BcN의 특성에 따라 취약성을 분류하기 위한 방법과 세부 분류 기준을 제시한다. 

3.1 BcN 서비스별 분류

BcN은 4개의 기술적 및 제어 계층의 단계별 분류(음성, 데이터 통합서비스와 유·무선 연동 및 통합서비스를 제공하는 1단계부터 시작하며, 제2단계 분류는 본격적인 플랫폼 보장 서비스, 가능한 빌미디어 영상 통합 및 회의 통합 서비스, 통신·방송·영상 통합서비스, 홈 네트워크 서비스 등)를 제공할 수 있다. 마찬가지로 서비스 및 제어계층 제3 단계에서는 1, 2단계 서비스는 물론 RAID/USN 서비스와 웹데스크탑 서비스까지 포함하는 전한 범위에 대한 제제공정 및 제어고객 결정을 갖춘 서비스를 제공하는 것을 목표로 하고 있다. 이로 이루어진 BcN 서비스는 세부로 정의되어 추가될 수 있는 가능성이 매우 크다. 따라서 ITX93와 같은 제첨진 8대 서비스(2.3GHz 휴대인터넷, DMX, 홀넷트워크, RFID, W-CDMA, 텔레메틱스, DTV, VoIP)와 3대 기반구조(BcN, IPv6, USN)를 기반으로 취약점을 분류하고 새로운 서비스 혹은 기반구조를 추가할 수 있도록 한다. 

ITX93의 8대 서비스 혹은 3대 기반구조에 대해 취약성을 분류하면 취약점은 보다세로 요구사항을 체계적으로 파악하
수 있으면 해당 서비스의 취약성을 일목요연하게 파악할 수 있고 보호보호요소기술판의 개발 필요성을 파악할 수 있는 기관이 된다.

32 보호대상범 분류
X.805 방법론에서 기초적인 취약성 분석 과정은 정보보호 계층별 공격을 분류기로 보호대상을 선행하고 이를 대상으로 수신승위 경로를 진행하여 보호보호요소기술판을 작성한다. 그리고 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 정보보호요소기술판을 작성하여 조치에 보호 대책을 강구할 수 있다. 또한 검증하기 위해 학문 DB와 연계하여 보호 대책이 제대로 강구되었는지 검증할 수 있다.

33 공격수단별 분류
시스템의 설계, 구현 및 운영 상에 존재하는 결함을 이용하는 공격수단에는 다음과 같은 것들이 있다.
- 장치의 물리적 위치 및 제거
- 장치 도용 및 위조
- 스나이핑(sniffing)
- 스파웃(spoofer)
- 재생(replaying)
- 트래픽 모나타링
- 보안 우회
- 세션 헬세키
- 강제 리셋
- 원격 코드 실행
- 필터링 크랙(cracking)
- 비밀 오버플로우
- 자원 고갈
- 백도어

이와 같은 수단 외에 다른 방법들을 추가할 수 있도록 고려한다.

3.4 대응방안별 분류
대응방안은 다음과 같은 X.805의 8가지 대책을 적용한다.
(1) 접근제어 : 비리가자가 정보통신시스템에 부정한 방법으로 접근하여 사용하는 것을 방지
(2) 인증 : 정보의 송수신자 또는 정보통신사 이용자의 식별 및 확인
(3) 보안 통제 : 사용자가 정보통신시스템을 통하여 정보를 송수신하거나 취학한 사실을 부인하는 것을 방지
(4) 데이터 결합성 : 정지 또는 보안준정 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 보안준정 정보를 인가되지 않은 방법으로 위조 또는 변조할 수 없도록 보호
(7) 가용성 : 네트워크 요소, 서비스, 응용을 적법한 사용 자들이 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) 패키 : 정보보여 네트워크 자원의 파괴
(2) 변조 : 비인가자에 의한 자원의 변조
(3) 도용 : 정보자 자원의 도용
(4) 유출 : 비인가자에 의한 자원 접근
(5) 중단 : 네트워크 자원 접근 방해

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

3.6 위협도별 분류
모든 취약성은 어떤 대상에 대한 것이지만, 어떤 영향을 미칠 것인가, 복구가 얼마나 걸리려 할 것인가 등 파급효과가 모두 다르면, 따라서 취약성을 파급효과 또는 위협도별로 분류할 필요가 있어 다음과 같이 세 단계로 분류한다.
(1) 고 : 보안 전반 또는 상당히 큰 규모의 망이 작동하지 못하거나, 서비스/구성요소 대부분이 정상 작동하지 못하는 등 파급효과가 큰 취약성
(2) 중 : 국지적인 망이 작동하지 못하거나 특정 보안 요소가 작동하지 못하는 등의 파급효과를 발생시키는 취약성
(3) 저 : 보호되어야 할 서비스/구성요소에 관한 정보가 유출되거나, 영향력이 적은 특정 장비가 오작동하는 등의 파급효과가 발생시키는 취약성

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

<표 1>은 이상의 경우와 취약성 분류 항목을 요약한 것이다. 이 분류 체계는 보안의 서비스 중 하나인 VoIP에 적용한 결과를 <표 2>에 나타내었다.

이상에서 제안한 분류체계가 기존의 분류 방법과 비교하면 <표 3>과 같다. 이 결과로 볼 때, 분 분문에서 제안하는 분류 체계는 기존의 방법보다 구체적이고 특히, 분류 구성 요소들의 간의 연관성을 제고하여 전체적인 보안 프레임워크를 마련하는데 매우 중요한 구실을 한다.
## 제 2) 분류 체계의 VoIP 적용 사례

<table>
<thead>
<tr>
<th>Layer/Plane</th>
<th>조화요소</th>
<th>목표값</th>
<th>공급단원</th>
<th>공급과정</th>
<th>목표</th>
<th>계산방법</th>
<th>적용대상소스</th>
<th>소프트웨어변경요소</th>
<th>실행체계변경요소</th>
<th>소프트웨어변경요소</th>
<th>적용대상소스</th>
<th>소프트웨어변경요소</th>
<th>실행체계변경요소</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP, Telnet, FTP</td>
<td>서버 대상 (S) 계층</td>
<td>2-3</td>
<td>서버 통신</td>
<td>서버로</td>
<td>서버</td>
<td>서버 통신</td>
<td>서버 통신</td>
<td>서버 통신</td>
<td>서버 통신</td>
<td>서버 통신</td>
<td>서버 통신</td>
<td>서버 통신</td>
<td>서버 통신</td>
</tr>
<tr>
<td>I, O, הארץ, 휴수</td>
<td>하장</td>
<td>상태</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
<td>휴수</td>
</tr>
<tr>
<td>네트워크 표준</td>
<td>FTPP</td>
<td>FTPP 내 네트워크 표준</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
<td>FTPP</td>
</tr>
<tr>
<td>TFTP</td>
<td>TFTP 내 네트워크 표준</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
<td>TFTP</td>
</tr>
<tr>
<td>DHCP</td>
<td>DHCP 내 네트워크 표준</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
<td>DHCP</td>
</tr>
<tr>
<td>SRP, H.333, MEGACO/1450, RSVP-1, SCP</td>
<td>SRP 내 네트워크 표준</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
<td>SRP</td>
</tr>
<tr>
<td>SEP, R.100</td>
<td>SEP 내 네트워크 표준</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
<td>SEP</td>
</tr>
<tr>
<td>HTTP</td>
<td>HTTP 내 네트워크 표준</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
<td>HTTP</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTPS 내 네트워크 표준</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
</tr>
<tr>
<td>IMAP</td>
<td>IMAP 내 네트워크 표준</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
<td>IMAP</td>
</tr>
<tr>
<td>SMTP</td>
<td>SMTP 내 네트워크 표준</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
<td>SMTP</td>
</tr>
</tbody>
</table>

## 제 3) 기준의 분류 방법과의 비교

<table>
<thead>
<tr>
<th>CVE</th>
<th>CC</th>
<th>대한 분류 체계</th>
</tr>
</thead>
<tbody>
<tr>
<td>목적</td>
<td>표준화된 취약점 설명</td>
<td>취약점 선정</td>
</tr>
<tr>
<td>형태</td>
<td>취약점 분석 결과</td>
<td>취약점 분석 및 대응에 필요한 기술 도구</td>
</tr>
<tr>
<td>브이크</td>
<td>일반</td>
<td>일반</td>
</tr>
<tr>
<td>적용대상</td>
<td>일반</td>
<td>일반</td>
</tr>
<tr>
<td>적용대상</td>
<td>일반</td>
<td>일반</td>
</tr>
<tr>
<td>적용대상</td>
<td>일반</td>
<td>일반</td>
</tr>
<tr>
<td>적용대상</td>
<td>일반</td>
<td>일반</td>
</tr>
<tr>
<td>적용대상</td>
<td>일반</td>
<td>일반</td>
</tr>
<tr>
<td>적용대상</td>
<td>일반</td>
<td>일반</td>
</tr>
<tr>
<td>적용대상</td>
<td>일반</td>
<td>일반</td>
</tr>
</tbody>
</table>
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 설명, 임계 경도, 서비스/기반 구조 ID, 서비스/기반 구조 이름, 서비스/기반 구조 설명, 위험 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, 위협도 ID, 위협도, 위협도 설명, 사용자 ID, 사용자 이름, 사용자 직급, 사용자 접근권, 사용자 접근권, 사용자 새스터드, 작업일시, 작업유형, 작업 유형, 작업 설명 등이다.

(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(기본키)
- 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.
· 작업유형 설명(work_description) : 각 작업유형에 대한 설명

(11) 변경이력(History) 객체
사용자가 취약성 DB에 접근, 입력, 수정, 삭제할 이력에 관한 객체이다.
· 취약성 ID : 취약성 객체를 참조하는 외래 키(복합키)
· 사용자 ID : 사용자 객체를 참조하는 외래 키(복합키)
· 작업일시(date) : 작업이 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 내 가지 정보가 입력, 관리된다. 첫째, 취약성 정보로서 IT809 8대 서비스 및 3대 기반구조에 대한 취약성 분석 결과 도출되는 정보들이 다.둘째, 8대 서비스 및 3대 기반구조에서 발생, 공개되는 취약성 정보들이 포함된다.셋째, 도출된 취약성을 보호하기 위해 요구되는 정보보호요구 사항 정보가 포함된다.넷째, 정보보호요구사항을 만족시키기 위해 필요한 정보보호 기술들이 포함된다.

이러한 네 가지 주요 정보들은 효과적으로 조작함으로써 제계적으로 정보보호프레임워크를 도출하고 상관관계를 잘 정리하여 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 혁신 기반이 될 공해양통합의 중요성과 보안 환경의 변화를 살펴보고, 이에 효과적으로 대응하기 위해 BcN의 취약성 분석하고 제계적으로 분류하기
의한 제거를 시한하였다. 또한, 광대역통합망에 대한 분석과 취약성 분석을 통해 도출된 취약성 정보를 체계적·관리할 수 있도록 데이터베이스를 설계하였다. 이 데이터베이스는 단순히 취약성만을 저장하는 것이 아니라 이를 검증하기 위하여 구체적 취약성 사례 데이터베이스와 연동하도록 설계되었다. 이로써 특정 서비스나 기반구조에 대한 취약성
을 도출하고 그에 연관된 사례들을 도출하여 직접 분석을 할 수 있도록 설계가 완료되었다. 또한 이 데이터베이스를 이용하여 실제 운영중인 서비스/기반구조에 대한 보안성 평가를 할 수 있게 되었다.

한편 이 데이터베이스에는 취약성을 보호/제거하기 위한 필요한 정보보호요구사항 및 정보보호보수기술 데이터베이스가 포함됨으로써, 새로운 구축형 서비스/기반구조에 대해서 정보보호회원업계 도출 과정에 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 점검하고 새로운 정보보호기술을 도출하는데 중요한 역할을 한 것으로 기대된다.

참고 문헌


윤종림
e-mail : abc@nilessoft.co.kr
1985년 충남사회학 전산학과(학사)
2001년 인포넷 주업연구원
2002년 ~ 현재 나일소프트 소프트웨어연구소 신임연구원
관심분야: 시스템보안, 네트워크보안, 보안 취약점

송영호
e-mail : yhsong@nilessoft.co.kr
1984년 한양대학교 산학협력을(학사)
1988년 연세대학교 전자통신학과(석사)
1984년 ~ 1994년 LG전자 컴퓨터사업부
화장/신임연구원
1998년 ~ 2000년 청신대전산과 교수
1994년 ~ 현재 나일소프트 소프트웨어연구소 연구소장
관심분야: 시스템보안, 위협관리, 컴퓨터포렌식

민병준
e-mail : bjmin@incheon.ac.kr
1983년 연세대학교 전자공학과(학사)
1985년 연세대학교 전자공학도(석사)
1991년 미국캘리포니아대학교(UC어바인)
전기및전자공학부(박사)
1984년 ~ 1989년 삼성전자 연구원
1992년 ~ 1994년 KT 신임연구원
1995년 ~ 현재 인천대학교 컴퓨터공학과 교수
관심분야: 보안, 유비쿼터스 컴퓨팅

이태진
e-mail : ttlee@kisa.or.kr
2003년 포항공과대학교 컴퓨터공학과(학사)
2003년 ~ 현재 한국정보보호진흥원 주임연구원
관심분야: 정보보호, 무선보안, 무선통신