ITU-T X.805 기반 네트워크 서비스 대상 정보보호프레임워크 도출 방법론

조영덕*, 원유재*
*한국정보보호진흥원 정보보호기술단 기술기획팀
e-mail: ydcho@kisa.or.kr

ITU-T X.805 based Vulnerability Analysis Method for Security Framework of End-to-End Network Services

Young-Duk Cho*, You-Jae Won*
*Information Security Technology Division, KISA
**Dept of Computer Engineering, Dae-sung University

요 약

본 논문에서는 종단간 신규 네트워크 서비스에 대한 ITU-T X.805 기반 취약성 분석과 정보보호 요구사항 및 보안 대책 도출 절차를 제시한다. 일련의 절차는 정보보호프레임워크 도출 방법론 혹은 방법론으로 줄여서 표현한다. 종단간 네트워크 서비스는 IT 839의 8대 서비스를 대상으로 하며 방법론은 ITU-T X.805 표준과 정보보호 컨설팅 방법론을 참고하였다. 방법론은 새로운 인프라나 서비스의 정보보호 대책을 설계하는데 필요한 도구로써의 역할을 하여 구축 단계부터 정보보호를 반영할 수 있는 분석틀을 제시할 것으로 기대한다.

1. 서론

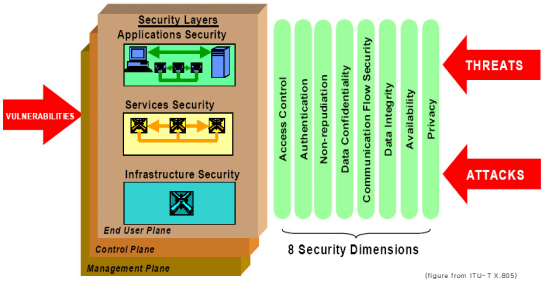
IT 839 정책으로 추진 중인 BcN(Broadband Convergence Network)은 유무선 인터넷 망 및 방송망까지 연동하여 광대역 고품질의 멀티미디어 서비스를 언제 어디서나 접속할 수 있는 기술을 의미한다. BcN 기반의 응용서비스로 우선 고려되는 것이 8대 서비스 - 휴대인터넷, VoIP, RFID, WCDMA, DMB, DTV, 텔레매틱스, 홈네트워크 - 이다. 이들 서비스들은 아직 본격적인 상용화 서비스가 보급되지 않은 상태로 서비스 제공이 우선 해결할 과제로 여겨지고 있지만 안정적인 서비스 제공을 보장하는 방안 역시 설계단계부터 고려해야할 몫이다. 특히 BcN 환경은 단일 지점 오류 발생으로 인해 망 전체로 피해가 급속도로 확산될 우려가 있으므로 보안대책 제공시 기존 오버레이 방식에서 망 구축 단계부터 임베드된 방식의 대책이 필요하다. 그러나 아직 구축되지도 않은 신규서비스에 대해 알려지지 않은 취약성과 위협을 검토하는 작업은 어느 정도 객관성의 한계를 갖기 마련이다. 이에 대하여 ITU-T X.805는 종단간 네트워크 서비스에 대한 정보보호 생명주기에 따른 정보보호 아키텍쳐 설계의 틀을 제공한다.

본 논문은 신규 출현 서비스의 설계단계부터 정보보호를 고려하여 반영할 수 있도록 ITU-T X.805 기반의 정보보호프레임워크 도출 방법론을 정의하고 있다. 방법론은 신규 서비스의 인프라/서비스/응용 계층별, 관리/제어/사용자 평면별 보호대상을 식별하고, 이들에 대한 위험분석을 통해 정보보호 요구사항과 대책을 도출하며 그 산출물을 정보보호프레임워크로 정의한다.

2. 관련 연구

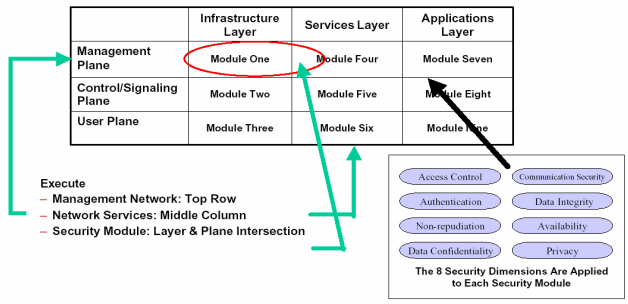
(그림 1)의 X.805는 ITU-T FG-NGN에서 NGN 정보보호 모델 개발을 위한 표준 규격으로 인용되고 있다. X.805는 크게 보안계층, 보안평면, 8개의 보안 서비스 개념으로 구성되어 있다. 보안계층은 네트워크 장치 및 시설들의 계층별 분류로 인프라 계층,

서비스 계층, 응용 계층으로 분류한다. 보안평면은 네트워크 행위별 분류로 관리 평면, 제어 평면, 사용자 평면으로 분류한다. 각 보안평면은 각 보안계층별로 적용하여 네트워크 서비스의 보호대상을 상세하게 분류·도출하게 된다. 정보보호 서비스는 네트워크 보호를 위해 제공되어야 하는 8가지 정보보호 기능 - 접근제어, 인증, 부인방지, 비밀성, 통신흐름 보호, 무결성, 가용성, 프라이버시 - 으로써 보호대상별로 적용하게 된다.



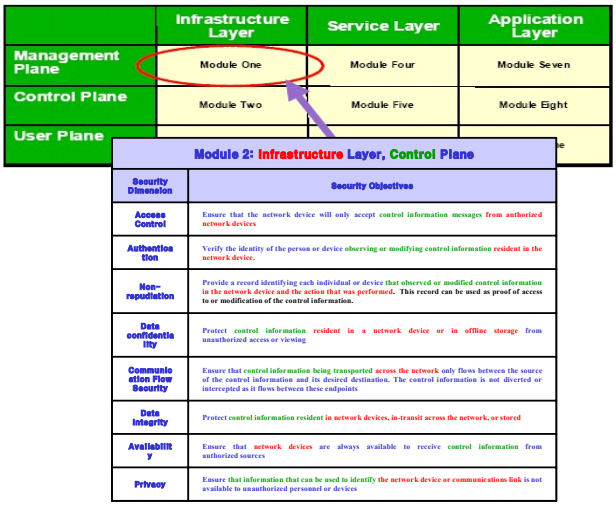
(그림 1) ITU-T X.805 정보보호참조모델

(그림 2)는 계층 및 평면별 도출된 9개 보호대상(모듈)별로 보안서비스를 적용하는 예를 보여주고 있다. X.805는 네트워크 서비스를 시스템적인 관점에서 분류·식별하므로 신규 출현 서비스처럼 아직 보안 개념조차 파악되지 않은 대상의 보호해야할 세부 자원을 도출하는 객관적인 도구로써 활용이 가능하다.



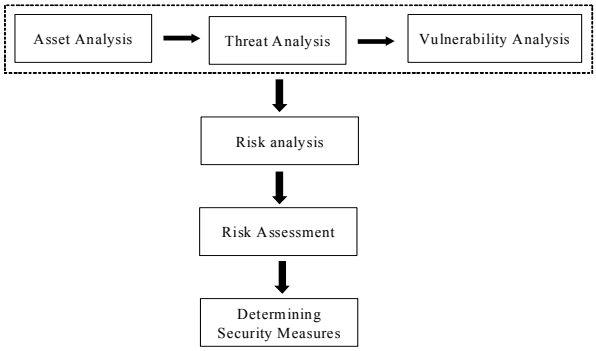
(그림 2) X.805의 계층별/평면별 정보보호 서비스 적용

(그림 3)은 (그림 2)에서 분류된 모듈별로 8개 보안서비스를 적용 했을 때 도출되는 정보보호 요구사항을 보여주고 있다. X.805에서는 9개 표로 표현된 모듈별 정보보호 요구사항의 템플릿을 제공하고 있다.



(그림 3) 보호대상별(모듈) 정보보호 요구사항 도출

방법론에서 참고하고 있는 또 다른 기술로써 정보보호 컨설팅 방법론이 있다. 컨설팅 방법론은 조직의 위험평가를 하는 방식에 따라 다소 차이는 있지만 일반적으로 (그림 4)와 같은 형식을 따르게 된다. 위험평가 방법론에는 BS7799, OCTAVE(Operationally Critical Threat, Asset and Vulnerability Evaluation), ISO 13335 GMITS(Guidelines for the Management of IP Security) 등이 있다.



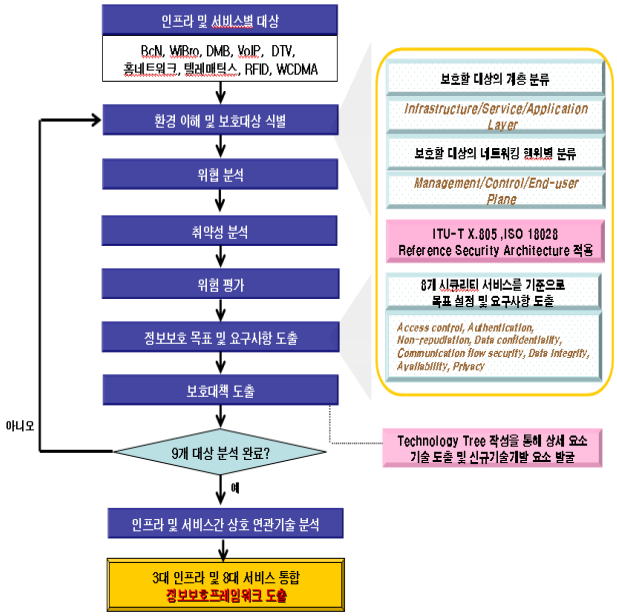
(그림 4) 일반적인 위험 평가 방법

3. ITU-T X.805 기반 정보보호프레임워크 도출 방법론

ITU-T X.805와 정보보호 컨설팅 방법론에서 착안한 정보보호프레임워크 도출 방법론은 (그림 5)로 요약할 수 있다.

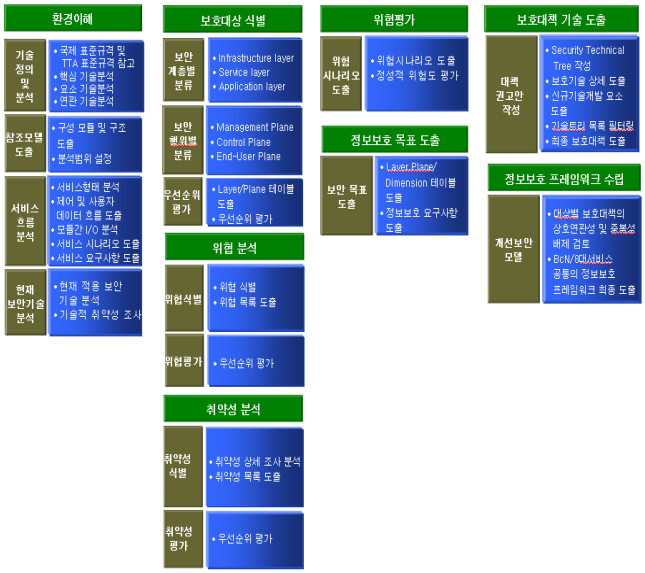
특정 서비스에 대한 환경이해와 보호대상 식별 태스크를 수행하고 보호대상별 위협요소를 예측하고, 현재 알려진 취약점을 조사한다. 이를 통해 위험 시나리오를 도출하는 등 정성적인 위험평가를 한 후 위험도에 따른 보호대상의 우선순위를 도출할 수 있

다. 높은 우선순위의 보호대상에 대해 X.805를 참조하여 정보보호 요구사항을 도출하고 이에 대한 보호대책을 수립함으로써 단일 신규서비스에 대한 정보보호 참조모델이 수립된다.



(그림 5) ITU-T X.805 기반 정보보호프레임워크 도출 방법론

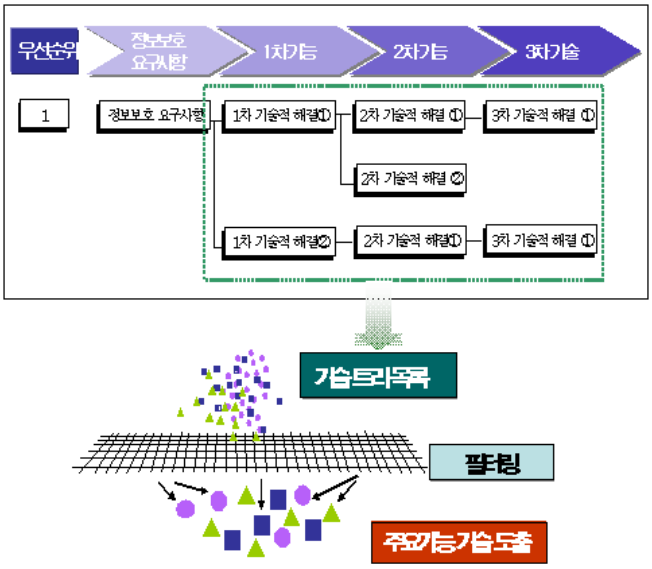
(그림 6)은 방법론의 태스크별 세부 내용을 나타낸다.



(그림 6) 방법론 세부 절차

X.805에서 보안 대책 수립을 위한 개념은 정보보호 요구사항을 통해 포괄적이고 추상적인 수준으로만 제공하고 있다. 이를 보완하기 위해서 제안한 방법론에서는 (그림 7)의 기술트리 전개법을 제안한다.

우선순위가 높은 정보보호 요구사항을 중심으로 현재 보안기술을 기본으로 단계별 대책을 도출한다. 브레인스토밍이나 전문가 활용을 통해 도출된 기술트리의 노드값 즉, 대책들에 대하여 기술개발 가능성 및 중요성, 지적재산권으로서의 가치 등을 고려하여 필터링하여 최종 보안 대책을 수립한다.



(그림 7) 기술트리 전개법

전체 프로세스는 정보보호 컨설팅 방법론과 유사하지만 제안한 방법론은 보호대상 식별을 위해 X.805의 보안계층과 평면, 서비스 개념을 도입하여 BcN 같은 다양한 인프라와 서비스가 공존하는 경우 특히, 신규서비스에 대한 정보보호 요구사항 등이 도출되지 않은 환경에서 정보보호 참조모델을 수립할 때 유용하게 활용가능한 장점이 있다.

4. 결론

국가적으로 추진 중인 IT 839의 신규 인프라와 서비스에 대해서 설계단계부터 정보보호를 고려할 수 있도록 객관적이고 조직적인 절차의 결과로써 정보보호 대책을 제시하기 위하여 본 방법론은 활용가능하다. 또한 동시적으로 신규 구축 중인 인프라와 서비스를 대상으로 통합 정보보호 모델 수립을 위하여 공동의 과제를 수행하는 산학연간 표준 업무 절차로써도 응용할 수 있다.

현재 한국정보보호진흥원에서는 제안한 ITU-T X.805 기반의 정보보호프레임워크 도출 방법론에 따

라 8대 서비스별 정보보호프레임워크를 관련 산학연간 협조 하에 개발하고 있다. 연내 도출될 서비스별 정보보호프레임워크는 정보보호기술개발 로드맵 및 신규 보안기술 도출 등에 광범위하게 활용될 것으로 기대하고 있다.

참고문헌

[1] ITU-T X.805, “Security Architecture for Systems Providing End-to-End Communications”

[2] S.Kim, J.Jee, T.Nam, S.Sohn, C.Park, "Framework of Network Security Service for Next Generation", Proceeding. WISA 2002, 123-130

[3] ITU-T SG17 Q.5, "ITU-T Rec. X.805 and its application to NGN", ITU-T FG-NGN Workshop Proceeding, 2005 April

[4] Korea Information Security Agency, "Vulnerability Analysis & Assessment Methodology version", 2002

[5] Kong, Luo, Xu, Gu, Gerla, Lu, "Adaptive Security for Multi-layer Ad-hoc Networks", Wireless Communications and Mobile Computing, Wiley Interscience Press, 2002

[6] Bass T., "Intrusion detection systems and multi-sensor data fusion", Communications of the ACM, vol.43, issue4, 2000 April