한국산학기술학회논문지
Vol. 10, No. 8, pp. 1911-1919, 2009

정보보호 시스템기반의 보안 수준 평가 도구(ISSPET) 개발

소우영[1], 김완경[1*], 김석수[2]
[1]한남대학교 컴퓨터공학과
[2]한남대학교 멀티미디어공학과

Development of Security Level Evaluation Tool(ISSPET) Based on Information Security System

Wooyoung Soh[1], Wankyung Kim[1*] and SeakSoo Kim[2]
[1]**Department of Computer Engineering, Hannam University**
[2]**Department of Multi-Media, Hannam University**

요 약 현재의 정보보호시스템 위험 분석 수준 측정에 대한 시험 평가업무는 미국, 영국을 비롯한 선진국에서만 평가 기술을 확보하고 있으나, 국내의 경우 위험분석 수준측정을 위한 인프라와 평가기술이 부족한 실정이다. 따라서 본 논문에서는 정보보안 위험분석 수준 측정 기술 및 평가방법에 대해 연구하고 이를 이용하여 보안통제항목의 개발 및 이를 적용한 보안 수준 성능 평가 도구를 제시한다. 제시한 도구를 이용한 정보보호 시스템의 보안 관리 수준 분석을 통해 현 시스템과 보안 환경에 대한 보안 관리 수준을 평가할 수 있을 것으로 기대된다.

Abstract Currently, the evaluation technology for the security systems of risk analysis level measurement is maintained by only the developed countries including U.S and U.K, and the evaluation technology and its infrastructure are insufficient for the evaluation technology of security threat analysis level measurement in Korea. Therefore this paper presents the development of the security control items and the evaluation tool(ISSPET) for the security level performance. It is expected to evaluate the security management level of the current system and its security environment through analyzing the security management level of security systems using ISSPET.

Key Words : Security Level Evaluation, Security Management

1. 서론

다양한 정보보호시스템 (Information Security System) 제품들이 사회 각 분야에서 구축·운영되면서 이에 따른 정보보호시스템들의 안전성 평가의 필요성이 증대되고 있다. 정보화 사회에 있어서 정보는 단순한 지식의 바탕이 되는 요소가 아닌 정치, 경제, 문화 등 사회 전반적인 중요한 자산이자 하나의 콘텐츠 자리 잡고 있다는 관점에서 볼 때, 정보보호시스템의 필요성은 필수적이라 할 수 있다.

정보보호시스템은 조직이 가지는 정보에 대한 무단 유출 및 파괴, 변조 등과 같은 공격에 대해 정보를 보호할 수 있는 원천적인 산물이라 할 수 있다. 그러나 조직의 정보보호 목표를 효율적이고 효과적으로 달성하기 위해서는 조직의 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준이나 평가모델이 필요하다. 또한 부문별 정보보호 수준을 평가하고 개선할 수 있는 평가방법론의 연구 역시 필요하다[1].

이와 맞물려 정보통신 시스템은 1950년대부터 평가 및 인증제도가 시작되었고, 소프트웨어 시스템의 경우에 ISO 9001과 같은 소프트웨어 품질 표준[2]이 제시되고 있으며, 정보보호시스템의 경우 ITSEC (Information

본 논문은 2009년도 한남대학교 교비학술연구조성비 지원에 의하여 연구되었음.
*교신저자 : 김완경(wankk12@hnu.kr)
접수일 09년 04월 22일 수정일 (1차 09년 05월 19일, 2차 09년 08월 12일) 게재확정일 09년 08월 19일

Technology Security Evaluation Criteria), TCSEC(Trusted Computer System Evaluation Criteria), CC(Common Criteria)등의 평가 기준이 등장하게 되고 이를 통해 정보보호시스템의 기술적 평가를 받게 된다. 국내의 경우 1996년 8월 제정된 정보화 촉진 기본법 제 15조 및 동법 시행령 제 15, 16조를 근거로 한국정보보호센터에서 K series(K0~K7)로 정보보호시스템에 대한 평가를 시행해 오고 있다.

그러나 흥미로운 사실은 높은 평가를 받은 정보보호시스템을 효과적으로 구축하여 운영한다할지라도 시스템을 보호하고 있는 환경이나 운용하고 있는 인력 수준에 따라서 위험성은 존재할 수밖에 없다. 일례로 정보화의 역기능 발생 사례를 살펴보면 무려 70% 이상이 기술적인 부분이 아닌 물리적, 환경적인 부분에서 발생된다[3].

물리적, 환경적인 부분에서 발생하는 정보화의 역기능을 줄이고, 그에 따른 물리적, 환경적 문제점을 파악하여 해결하기 위해 미국을 비롯한 세계 각국에서는 조직의 정보보호시스템에 대해 물리적, 환경적인 부분을 포함하여 전반적인 사항을 다루고 있는 정보보호관리 (ISM : Information Security Management) 체계를 갖추고 있다. 정보보호관리 체계를 갖추기 위해서는 정보보호시스템에 대한 위험 분석 수준 측정에 대한 시험·평가가 선행되어야 하나, 이는 미국, 영국 등 몇몇 선진국에서만 평가 기술을 확보하고 있으며, 국내의 경우 위험분석 수준측정을 위한 인프라와 평가기술이 부족한 실정이다[4].

따라서 본 논문에서는 정보보안 위험분석 수준 측정 기술 및 평가방법에 대해 연구하고 이를 이용하여 보안 통제항목의 개발 및 이를 적용한 보안 수준 성능 평가 도구를 제시한다.

본 논문의 2장에서는 국내외 정보보호 관리 기준들에 대해서 비교•분석하고 3장에서는 자체수준 위험 분석을 돌출하여 종합 평가 기준을 수립한다. 4장에서는 정보보호시스템 성능평가 도구(ISSPET : Information Security System Performance Evaluation Tool)를 구현하며 5장에서 결론 및 향후 연구 방향으로 끝을 맺는다.

2. 관련 연구

2.1 국내·외 정보 보호 관리 기준

정보 보호 관리는 위험 관리의 상위 개념이며 위험 관리는 위험 분석의 상위 개념으로 하위 개념들을 모두 포함한다. 정보 보호 관리는 조직의 정보 시스템에 대한 전반적인 사항을 다루며 정보보호에 관련된 업무를 몇 개의 통제 분야(클래스)로 나누고 각 통제 분야별로 다수의 통제 대책(컴포넌트)으로 구성된다. 이러한 정보 보호 관리 기준들의 예로 국제표준인 ISO/IEC[5] 영국 BSI의 BS7799[6] (ISO/IEC 17799 : 2000은 Part 1이 국제 표준으로 인정된 것임)와 카네기 멜론 대학의 SSE-CMM[7], ISO/IEC 13335(Guidelines for the Management of IT Security : GMITS)과 국내의 정보보호 관리 기준 등이 있다[8].

국내·외 정보 보호와 관련한 기준들이 많이 있지만 앞서 설명한 것과 같이 물리적, 환경적인 부분까지 고려하여 평가가 이루어지는 즉, 전사적으로 보안 수준을 점검할 수 있도록 제시하고 있는 기준들은 BS7799나 국내의

[표 1] 국내·외 관리 기준 비교

구분	관리기준(국내)	ISO/IEC 13335	BS7799	SSE-CMM
작성기관	KISA	ISO/IEC JTC1	영국 BSI	미국 ISSEA
특징	-BS7799를 국내 실정에 맞도록 문서화 -BS7799보다 교육 훈련 부분을 구체화하고 일부분을 축소시킴	-여러 표준 문서에서 자료를 수집하여 이를 체계적으로 정리한 보고서로 지침 성격을 가짐 -조직이 보유한 정보자산이 주요 대상	- 정보보호 관리체계를 효율적으로 수립, 수행, 감시하기 위한 방법론 제시 - 조직 상호간의 신뢰성 있는 거래를 위한 기준	-ISO/IEC 12207에 기초한 IT 정보보호프로세스 성숙도 측정 -정보보호관리 지침에 보조적으로 사용가능
작성년도	2001	1996	1999	1999.4
작성목적	정보보호관리 체계 수립/인증	IT 보호관리	정보보호관리 체계 수립/인증	IT 시스템 보호관리
적용범위	전사적	IT	전사적	IT 시스템
통제사항분류	13개 분야	조직적&물리적 7개 분야 IT 시스템분야 5개 분야	10개 분야	기본/프로젝트 및 조직 22개 분야
통제사항 수	131개	63개	127개	123개

정보보호 관리 기준 정도이다.

ISO/IEC 13335(GMITS)의 경우는 기본적으로 IT 보호 관리를 목적으로 작성되었고, 조직이 보유하고 있는 정보 자산이 주요 대상이라고 볼 수 있다. 또한 카네기 멜론 대학의 SSE-CMM의 경우는 IT 정보 보호 프로세스에 매핑 시켜 성숙도를 측정하는 수단으로 이용하기 때문에 기존의 프로세스들이 오래 동안 적용되면서 프로세스들의 성숙도를 측정하고 분석하는 것이다. 따라서 기본적으로 정보 시스템 구축 정도가 오래 되지 않은 우리나라 실정에서는 맞지 않다.

표 1은 국내·외 관리 기준들에 대해 비교 분석 한 것으로써[9], BS7799의 경우는 '인증'과 연결되어 활용되기는 하지만 인증만을 목적으로 하는 것이 아니라 광범위하고 총체적인 'Best Practice'를 제시하여 정보보호 관리를 실행함에 있어서 평가 지표나 적절한 대책 선택을 위한 방법으로 활용 될 수 있다. 또 국내의 정보보호 관리 기준 역시 이러한 BS7799의 수준을 프로세스별로 내용을 더하거나 삭제하여 우리나라의 수준에 맞도록 수정한 것이다.

2.2 정보보호시스템의 평가 방법

본 절에서는 국내외 여러 평가 방법 중, 1999년 6월 국제표준(ISO/IEC)으로 승인된 CC기반의 평가 방법을 기준으로 분석한다. CC는 모든 보안제품에서 필요로 하는 보안기능의 전체집합을 클래스-패밀리-컴포넌트-엘리먼트로 보안기능에 대한 구현의 정확성에 대한 보증요구사항의 전체집합을 계층적으로 분류하였고 7단계의 보증수준별로 요구하는 보증 요구사항(컴포넌트)을 정의하고 있다[10].

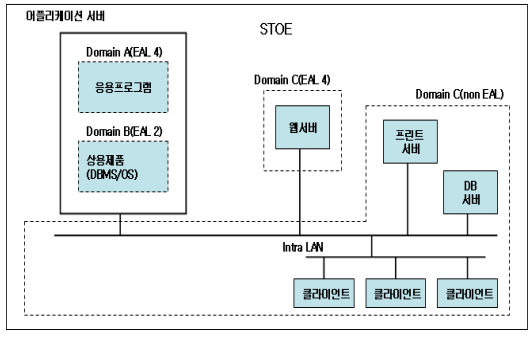
각 보증수준 간에는 완전성, 엄격성 및 정형성 관계를 갖는다. 정보보호시스템의 제품유형에 따라 CC 보안기능요구사항의 일부를 선택하고 7단계의 보안수준 중 하나를 택하여 PP(Protection Profile) 또는 ST(Security Target)를 구성한다[11]. ISO/IEC는 CC의 PP와 ST를 기반으로 SPP(System Protection Profile)와 SST(System Security Target)[12]의 개념을 제공하며, 이는 운용시스템에 대한 환경과 정보기술등을 평가하기 위한 기준이다. SPP와 SST를 기준으로 ISO/IEC에서는 해당 운영시스템에 필요한 보안수준을 형성하는 과정을 다음과 같이 크게 3단계로 나누어 평가한다.

- 보안위험이 운영시스템에 적용가능한지를 결정하기 위한 위험평가
- 보안통제 선택, 평가 등을 통해 위험을 대체, 소멸하기 위한 위험 경감
- 평가 후 운영시스템에 존재하는 잔여위험이 실제 운영 환경에 적합한가를 확인하는 인가

통상 운영시스템을 평가하기 위해서는 운영시스템의 환경 분석이 선행되어야 하므로, 해당 운영시스템의 문제점과 해결책을 먼저 고려해야 한다[13]. 예를 들어, 운영시스템을 구성하는 정보보호시스템의 업데이트, 운영장비들의 교체 등은 전체 운영시스템에 영향을 미치기 때문에 이에 따른 구성목록(Configuration list)를 만들어 그 운영시스템의 범위를 식별해야 한다[14].

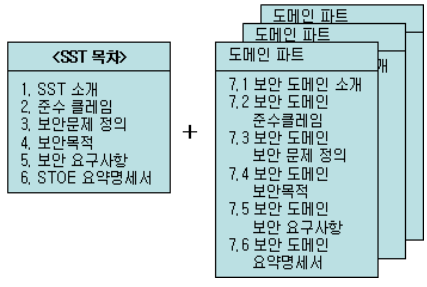
2.3 평가되지 않은 시스템의 평가 방법

안전한 제품(평가받은 제품)은 운영 시스템 보안에 중요한 공헌을 제공하며, CC로 평가된 제품을 사용하면 안전한 운영시스템을 구축을 할 때 유리하다. 그러나 그림 1과 같이 운영 시스템내의 제품들은 모든 제품들이 CC 평가를 받지 않은 제품으로 구성될 수 있다[12].



[그림 1] 운영시스템의 구조

ISO/IEC 19791에서는 운영시스템 내에 각 제품의 특성에 따라 유사한 보안정책을 가지는 제품을 Domain이란 단위를 적용을 하여, SST 평가 그림 2에 평가되지 않는 제품들을 적용한다[12].



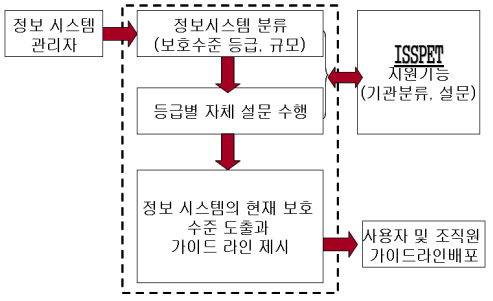
[그림 2] ISO/IEC 19791의 SST 목차

3. 자체수준 위험분석

본 장은 정보시스템의 관리자가 자체적으로 정보보호 관리 활동 및 정보자산의 보호조치 상태 등을 진단하고, 정보보호 조치가 부족한 부분과 그에 대한 가이드라인을 권고 받을 수 있도록 자체수준 위험분석 진단에 대한 연구이다. 본 장의 평가 기관 분류 및 기준 등은 국가정보원에서 발행하는 '국가 사이버 안전 매뉴얼-부록편'을 기준으로 한다. 다음 그림 3은 전체적인 위험분석 프로세스를 나타낸 것이며 정보보호시스템 성능평가 도구인 ISSPET에 대해서는 다음 장에서 논한다.

3.1 정보시스템 분류 기준

표 2는 정보시스템 분류의 기준은 수행업무의 중요도, 정보시스템 및 정보의 중요도 그리고 피해분석 등 크게 세 부분으로 구성되어 있으며[15], 각 기관 분류 기준에 따른 평가 요소를 분류하였다.



[그림 3] 자체수준 위험 분석 프로세스

[표 2] 기관분류 기준 및 평가요소

기관 분류 기준	평가요소	
수행업무의 중요도	수행무의 국가사회적 중요도	국가안전보장과의 연관성
		사회질서 유지와의 연관성
		국가 경제이익 보호와의 연관성
		국민생명 보호와의 연관성
	인원 및 서버 규모	
정보시스템 및 정보중요도	정보 중요도	
	정보시스템 의존도	
	대외업무연계 정도	
피해 분석	위협발행 가능성	
	피해영향 정도	

[표 3] 기관분류 기준표

분류기준	평가요소	평가점수			가중치	평가수준
수행업무의 중요도	수행업무의 국가사회적 중요도	VH	H	M	3	A급: 31~39 B급: 21~30 C급: 13~20
		3	2	1		
	인원 및 서버 규모	VH	H	M	1	
		3	2	1		
정보시스템 및 정보중요도	정보중요도	VH	H	M	3	
		3	2	1		
	정보시스템 의존도	VH	H	M	1	
		3	2	1		
	대외업무연계 정도	VH	H	M	1	
		3	2	1		
피해분석	위험발생 가능성	VH	H	M	2	
		3	2	1		
	피해영향 정도3	VH	H	M	2	
		3	2	1		

3.2 정보시스템 분류 방법

정보시스템 분류 기준의 세부요소에 대하여 상-중-하로 평가하고 여기에 가중치를 곱하여 총점을 산정하여, 정보시스템을 '가'급, '나'급, '다'급으로 분류하였다. 다음 표 3은 기관분류 기준표를 나타낸 것으로써 분류기준과 평가 요소에 따른 가중치를 주고 이에 따른 평가 수준을 수치적으로 표시한 것이다.

기관분류를 위한 총평가점수를 T, 각 평가요소별 점수를 Ei, 평가요소별 가중치를 Wi라고 하면 총점에 따른 기관(정보통신망) 분류는 아래와 같다.

$$T = \sum_{i=1}^{7} E_i \times W_i$$

'가'급 기관: $31 \leq T \leq 39$

'나'급 기관: $21 \leq T \leq 30$

'다'급 기관: $13 \leq T \leq 20$

3.3 점검 항목

효율적인 보안관리를 위해서 점검항목을 A, B, C 항목으로 분류하였으며, 각 정보시스템 분류에 따라 차등적으로 적용하도록 하며 각 정보시스템이 적용되어야 할 사항은 다음과 같다.

A 항목: 모든 정보시스템이 필수적으로 수행해야 할 항목
B 항목: 중요 정보통신망을 운영하는 정보시스템이 추가로 수행해야 할 항목
C 항목: 매우 중요한 정보통신망을 운영하는 정보시스템이 수행해야 할 항목

즉 기관분류 결과에 따라 다음과 같이 차별화된 점검항목을 적용한다.

'A'급 정보시스템: A, B, C 항목을 모두 적용
'B'급 정보시스템: A, B 항목을 모두 적용
'C'급 기관: A 항목을 모두 적용

3.4 보안 관리 수준 평가 방법

3.4.1 점검분야별 평가

해당기관의 등급에 따라 점검항목 구성을 하였으며, 각 점검항목별로 수행(Y) 또는 미수행(N)으로 점검결과를 평가를 실시한다. 해당사항이 없는 점검항목은 해당사항 없음(N/A) 표시한다. 예를 들면, NUM(a)는 점검결과 사 'a'인 점검항목의 개수이다. 점검분야별 평가점수(T_j)를 다음과 같이 산정한다.

$$T_j = \frac{NM(Y)}{NM(Y)+NM(N)} \times 100$$

점검분야별 평가점수(T_j)를 이용하여 등급 평가

$$\Rightarrow \begin{array}{l} 90\% < T_j \leq 100\% : \text{최우수} \\ 80\% < T_j \leq 90\% : \text{우수} \\ 70\% < T_j \leq 80\% : \text{양호} \\ 60\% < T_j \leq 70\% : \text{미흡} \\ 70\% < T_j \leq 60\% : \text{불량} \end{array}$$

3.4.2 점검분야 누적 합산

각급기관의 정보보안업무 환경에 따라 점검분야는 총 9개 분야로 구성되어 있으며, 각급기관의 정보보안업무 환경에 따라 각 점검분야의 중요도도 달라질 수 있다. 그러므로 아래의 예 표 4와 같이 점검분야에 대한 우선순위를 자체적으로 결정하고 순위별 가중치 계수를 참조하여 보안관리수준 종합평가에 반영한다.

점검 분야별 가중치(λ_j)를 이용하여 다음과 같이 당해 기관의 점검분야별 평가점수를 합산하여 누적평가 점수(Φ)를 산출(Λ는 가중치 총합)한다.

$$\Phi = \sum_{j=1}^{n} \frac{T_j \times \lambda_j}{\Lambda}, \qquad \Lambda = \sum_{j=1}^{n} \lambda_j$$

* T_j : *점검분야 대분류별 점수*, n : *점검분야 총 개수*

[표 4] 점검분야별 정보보안 우선순위에 따른 가중치

점검분야별 정보보안 요구수준	우선순위	가중치 (λ_j)
정보보안 관리체계	1	1.4
정보보안계호기 및 활동	8	1.3
정보자산통제	2	1.2
인적보안	6	1.1
물리적보안	6	1.0
접근 보안대책	3	0.9
운영관리	4	0.8
시스템 개발 및 유지보수	5	0.7
보안시스템	1	0.6

3.4.3 종합 평가

평가 방법은 각급기관별 분야별 점검사항에 대한 평가점수를 누적 합산한 값(Φ)과 각급기관의 정보보안업무 활동 정도를 반영하기 위해 전체 점수의 5%범위 내에서 평가된 점수(α)를 가·감산하여 종합평가 점수를 산정한다.

종합평가 점수산정의 순서를 정리하면 다음과 같다.

- 기관분류 방법 및 기준에 따라 등급(가, 나, 다) 결정한다(요구사항 위험분석 모드).
- 분류 등급에 따라 점검항목 결정한다.
- 점검항목에 따라 분야별로 평가한다.

분야별	분야1	분야2	분야3	...	분야n
평가	T_1	T_1	T_3	...	T_n

- 분야별로 평가에 가산치를 합산하여 누적 점수를 계산한다.

분야별 누적합산	$\varnothing = \sum_{j=1}^{n} \frac{T_j \times \lambda_j}{\Lambda}$

- 분야별평가 누적 점수를 95%로 환산하고, 각급기관 정보보안 활동 정도 점수(5%내)를 합산하여, 종합평가 점수를 결정한다.

종합평가 점수	$Z = 0.95 \times \Phi + \alpha$

- 종합평가 점수(Z)에 따라 5개 등급으로 보안관리 수준을 평가한다.

90% < Z ≦ 100% : 최우수
80% < Z ≦ 90% : 우수
70% < Z ≦ 80% : 양호
60% < Z ≦ 70% : 미흡
50% < Z ≦ 60% : 불량

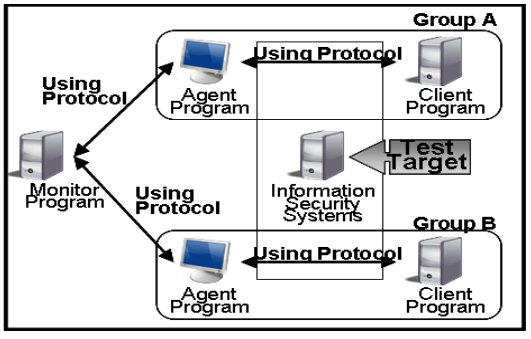
4. ISSPET 설계 및 구현

본 장에서는 3장에서 제시한 평가 기준을 적용하기 위한 ISSPET를 설계 및 구현한다. ISSPET는 오픈소스인 스노트를 기반으로 하며, MySQL에 룰 파싱 정보를 실시간으로 저장한다. 즉, ISSPET는 해당 시스템의 자체 수준 평가 결과를 돌출하기 위한 수단으로써의 실시간 운영시스템으로 활용하기 위해 설계한다.

4.1 전체 시스템 구성

본 논문에서 제시하는 ISSPET는 스노트 룰을 이용하여 공격에 대한 정보를 수집하고, 이를 이용하여 공격 패킷을 생성하여 해당 시스템에 전송하게 된다. 그리고 전송된 결과를 수집하여 사용자에게 전송결과를 모니터링 할 수 있도록 한다. 그림 4는 본 논문에서 제시하는 정보보호 시스템 성능 평가 시험 도구인 ISSPET의 전체 구성도이다.

ISSPET의 모니터 프로그램에서 공격에 대한 정보를 선택하여 에이전트 프로그램으로 명령을 하달한다. 명령을 받은 에이전트 프로그램은 UDP인 경우 공격 패킷을 생성하여 바로 전송하게 되고, TCP인 경우 3웨이 핸드쉐이킹을 통해 TCP연결을 수행한 후 공격 패킷을 전송하게 된다. 클라이언트 프로그램은 로그기록을 살펴보다가, 공격 패킷에 대한 정보가 로그에 남으면 이를 에이전트 프로그램을 통해 모니터 프로그램으로 전송한다. 모니터 프로그램은 전송된 결과를 수집하여 해당 성능평가에 대한 결과를 출력한다.

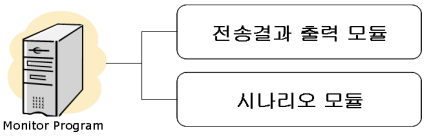


[그림 4] 정보보호 시스템 성능평가 시험도구의 전체 구성도

4.2 모니터 프로그램

모니터 프로그램은 사용자가 명령을 내리고, 결과를 볼 수 있는 콘솔로 사용된다. 그림 5의 모니터 프로그램은 크게 시나리오를 작성하여 에이전트에 전송하는 시나리오 모듈과 클라이언트로부터 오는 전송결과를 수집하여 분석, 결과를 출력하는 전송결과 출력 모듈로 나눌 수 있다.

시나리오 모듈에서의 시나리오는 공격에 대한 Key값으로 이루어져 있으며, Key값에 대한 정보는 에이전트에서 데이터베이스로 접속하여 데이터를 가져오게 된다. 따라서 시나리오 모듈은 데이터베이스를 관리하는 기능을 가지고 있다. 공격에 대한 데이터베이스는 스노트의 룰에서 추출한다.



[그림 5] 모니터 프로그램

[그림 6] 에이전트 프로그램

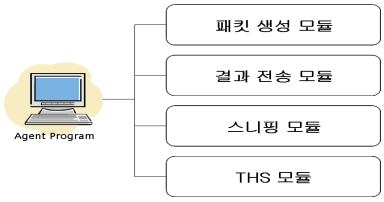
4.3 에이전트 프로그램

아래 그림 6의 에이전트 프로그램은 작성된 시나리오를 바탕으로 공격에 대한 패킷을 생성하여 해당하는 클라이언트 프로그램으로 전송하는 역할을 담당하는 부분이다.

본 논문에서는 실제 네트워크 환경이 다일 도메인이 아닌 여러 도메인이 운영된다는 점을 감안하여 다중 도메인 환경에 대한 정보보호시스템 시험평가를 위해 하나의 에이전트 프로그램이 여러 개의 IP주소를 가지고 있는 것처럼 보이기 위해 패킷을 스니핑하는 모듈이 추가하고, TCP프로토콜을 이용하는 공격을 위해 스니핑 된 정보를 이용한 IP 스푸핑 기술로 3-way 핸드쉐이킹을 하는 모듈도 추가한다.

4.4 클라이언트 프로그램

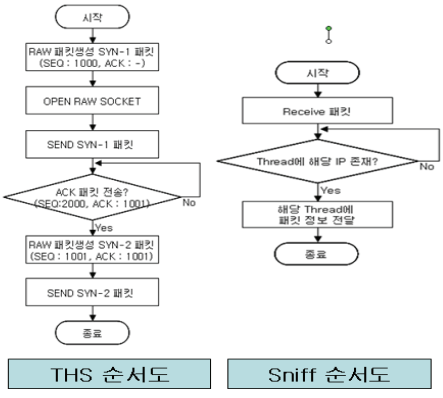
그림 7의 클라이언트 프로그램은 테스트 하고자 하는 정보보호 시스템들의 뒤편에 있는 시스템에 설치하는 프로그램이다. 이를 이용하여 에이전트 프로그램에서 전송하는 공격에 대한 수신여부와 탐지여부를 파악할 수 있다.



[그림 7] 에이전트 프로그램

먼저 클라이언트 프로그램은 자신에게 전송되어지는 공격에 대한 결과를 수집한다. 또한 정보보호 시스템들의 로그를 분석하여 본 공격이 탐지가 되었는지 여부를 수집한다. 이렇게 수집된 결과들은 에이전트 프로그램에게 전송되어 지며, 전송되어진 결과는 에이전트 프로그램이 수집하여 모니터 프로그램에게 전송하여 출력되어진다.

THS 모듈은 TCP 프로토콜을 사용하는 공격을 위한 모듈로 클라이언트와 RAW소켓을 사용하여 수행한다. 연결이 완료되면 공격에 대한 패킷을 전송하게 되며, THS모듈은 Sniff모듈과 함께 동작한다.



[그림 8] THS와 Sniff 순서도

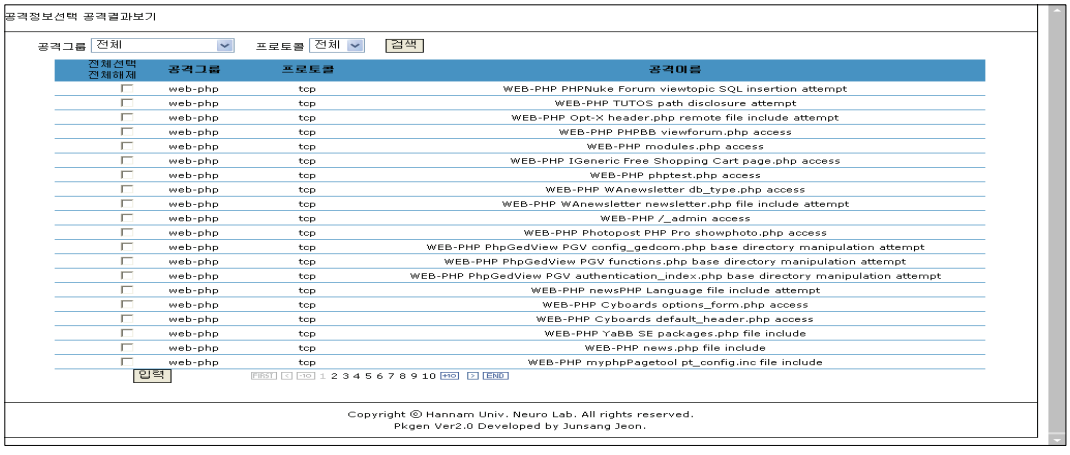
4.5 ISSPET GUI

본 시험도구는 GUI의 역할을 위해 PHP와 MySql을 사용하여 구현하였다. GUI는 콘솔부분에 해당하며, 룰 정보를 파싱하여 MySql DB에 저장한다. 저장되는 정보들은 크게 3가지 테이블에 저장되며, 그 테이블은 그림 9와 같이 공격정보이름, 헤더정보, 옵션정보로 나누어진다.

```
| Field       | Type         | Null | Key | Default | Extra          |
| a_id        | int(11)      |      | PRI | NULL    | auto_increment |
| attack_name | varchar(100) |      |     |         |                |
mysql> desc attack_header_tb;
| Field    | Type         | Null | Key | Default | Extra          |
| t_id     | int(11)      |      | PRI | NULL    | auto_increment |
| a_id     | int(11)      | YES  |     | NULL    |                |
| protocol | varchar(10)  | YES  |     | NULL    |                |
| s_addr   | varchar(100) | YES  |     | NULL    |                |
| s_port   | varchar(10)  | YES  |     | NULL    |                |
| d_addr   | varchar(100) | YES  |     | NULL    |                |
| d_port   | varchar(10)  | YES  |     | NULL    |                |
| direct   | char(2)      | YES  |     | NULL    |                |
| msg      | varchar(255) | YES  |     | NULL    |                |
9 rows in set (0.00 sec)
mysql> desc attack_option_tb;
| Field        | Type         | Null | Key | Default | Extra          |
| o_id         | int(11)      |      | PRI | NULL    | auto_increment |
| t_id         | int(11)      | YES  |     | NULL    |                |
| a_id         | int(11)      | YES  |     | NULL    |                |
| option_name  | varchar(20)  | YES  |     | NULL    |                |
| option_value | text         | YES  |     | NULL    |                |
5 rows in set (0.00 sec)
```

[그림 9] 룰 정보 파싱 정보

각각의 테이블은 key값으로 조인되며, 이를 이용하여 데이터를 추출할 수 있으며, 그림 10의 ISSPET GUI환경에서 테이블에 저장된 정보를 이용하여 룰을 선택하고 선택된 룰을 이용하여 공격에 대한 시나리오를 작성하게



[그림 10] ISSPET GUI 환경

된다. 선택된 룰은 key값만을 전달하며, 전달된 key값을 이용하여 헤더와 옵션정보를 가져오게 된다. 본 논문에서 개발한 ISSPET를 이용하여 해당 네트워크와 정보보호 시스템에 공격 패킷을 생성하여 이를 전송하면, 보안 수준 평가 기준에 따른 결과가 수집되며, 이를 이용하여 네트워크 정보보호 수준 시험 평가에 적용 시킬 수 있다.

6. 결론

대부분의 조직이 분산 네트워크를 통해 이루어지고 있음을 감안한다면 전반적인 네트워크 시스템의 구축환경과 정보보호 시스템의 성능 평가가 반드시 필요하다. 현재 국제공통표준인 CC(Common Criteria)나 CC인증 민간 평가기관을 해당 시스템의 안정성과 보안성 등을 평가 받을 수 있다. 그러나 이를 통해 해당 시스템이 높은 보안성과 안정성을 보증하는 평가 결과를 가진다고 하더라도 평가를 하는 평가기관의 운영환경과 실제 시스템이 적용될 환경과 시스템 운영 인력이 반드시 일치하지는 않는다. 이는 외부로부터의 위협요소가 때에 따라 급변하기도 하며, 시스템의 운영 환경 또한 계속적으로 바뀔 수 있기 때문이기도 하다. 위와 같은 문제점을 해결하기 위해 실제 운영환경에 따른 성능 평가에 대한 연구가 활발히 진행 중이며, 본 논문에서는 오픈 소스인 스노트를 이용한 정보보호 시스템을 대상으로 실시간으로 평가 할 수 있는 보안 수준 평가 도구인 ISSPET를 설계 및 개발하였다. ISSPET의 평가 기준은 국정원에서 제시하는 국가 사이버안전 매뉴얼을 바탕으로 하였으며, 이를 이용하여 현 조직의 정보보호 수준을 평가 할 수 있을 것으로 사료된다. 그러나 정확한 정보보호 수준을 평가하기 위해서는 현재 정보시스템의 이용자와 관리자등의 정보보호 수준을 평가할 수 있는 지표가 선행되어야 할 것이며, 이러한 정보보호 수준 평가 지표에 대한 객관적인 결과를 얻기 위해서는 표준화된 지표가 필요하다. 또한 해당 시스템의 구축 환경에서의 사용자, 즉 구성원들의 설문조사가 함께 병행되어야 할 것이다.

참고문헌

[1] 강신원, 국가정보화지수 측정을 위한 가중치 연구 : RCSS를 중심으로, 정보통신정책연구 제6권 제 2호, 1999.

[2] 김기윤, 나관식, “취약성 평가에 의한 정보보호지표의 계량화 : 정보자산가치가중치법”, 통신정보보호학회지 제10권 제1호, 2000.

[3] 이강신 외, “국내외 정보보호 관리 모델에 관한 고찰”. 정보보호학회지 제11권 제3호, pp24-37, 2001.

[4] 김정덕 외, “위험 분석 도구 기초 기술 개발에 관한 연구”, ETRI보고서, 2001.

[5] ISO/IEC JTC1/SC 27/WG 3, ISO/IEC TR 19791 v2.0, http://www.gammassl.co.uk/ist33/27N4246.pdf, June 30, 2005.

[6] BSI(1999), BS7799, BSI.

[7] SSE-CMM, "Project, Systems Security Engineering Capability Maturity Model(SSE-CMM) - Model Description Document," V.2, 1999. 4.

[8] 박현우 외, “정보 시스템을 위한 범용 웹기반 위험분석 프로세스," 2002 한국 디지털 컨텐츠 학회 학술대회(DCS 2002) 논문집, Vol.3, 2002. 12, pp205-209.

[9] 박준형 외, “웹기반 보안 관리 수준 분석 도구”, 한국정보처리학회 2003년 춘계학술대회, Vol 10 No. 01 pp1677~1680, 2003.05.

[10] Kabseung Kou, "Comparative Study on Information Schema Evaluation", ICHIT, Vol 02, pp473~481, 2006.

[11] CC, “Common Criteria for Information Technology Security Evaluation, Version 3.0,” CCMB-2005-07-001, July, 2005.

[12] ISO/IEC TR 15446, “Information technology-Security techniques-Guide for the production of protection profile and security targets”, July 2, 2004.

[13] Haruki Tabuchi, “Business aspect of security evaluation and CCRA”, June, 2005.

[14] Hirohisa Nakamura, “Evaluation of application systems by ISO/IEC TR 19791,” September, 2005.

[15] 이강수 외, “유비쿼터스 환경에서의 위험분석 수준 측정 도구 개발”, RIC 보고서, 2008.

소 우 영(Wooyoung Soh) **[정회원]**

- 1979년 2월 : 중앙대학교 전자계산학과 (이학사)
- 1981년 2월 : 서울대학교 전자계산학과(이학석사)
- 1990년 1월 : 미국 매릴랜드대학교 전자계산학과(이학박사)
- 1996년 1월 ~ 12월 : 한국전자통신 초빙연구원
- 1991년 9월 ~ 현재 : 한남대학교 컴퓨터공학과 교수

<관심분야>
컴퓨터 보안, 네트워크 보안, 정보보호 시스템

김 완 경(Wankyung Kim) **[정회원]**

- 2003년 2월 : 한남대학교 컴퓨터공학과 (공학사)
- 2004년 8월 : 한남대학교 컴퓨터공학과(공학석사)
- 2008년 8월 : 한남대학교 컴퓨터공학과(박사 수료)
- 2008년 3월 ~ 현재 : (주)휴메이트 연구원

<관심분야>
무선 네트워크 보안, 시스템 보안, 정보보호 시스템

김 석 수(SeakSoo Kim) **[종신회원]**

- 1991년 2월 : 성균관대학교 대학원 (공학석사)
- 1991년 1월 ~ 1996년 5월 : (주)정풍물산 중앙연구소 주임연구원
- 1997년 3월 ~ 1998년 2월 : 한국 탑웨어 책임연구원
- 1998년 3월 ~ 2000년 2월 : 경남 도립 거창전문대학교 교수
- 2000년 3월 ~ 2003년 2월 : 동양대학교 컴퓨터공학부 교수
- 2002년 2월 : 성균관대학교 대학원 (공학박사)
- 2003년 3월 ~ 현재 : 한남대학교 멀티미디어공학 교수

<관심분야>
상황인지, uHealthcare, SCADA, 정보보안