보안위험분석을 위한 평가기반 CBR모델
(The Evaluation-based CBR Model for Security Risk Analysis)

방 영 환 † 이 강 수 ††
(Young-hwan Bang) (Gang-soo Lee)

요 약 정보시스템을 이용하는 금융, 무역, 의료, 에너지, 교육 등 사회 각 분야에서 정보화가 급속하게 진전되고 있다. 정보시스템에 대한 보안관리는 위험분석평가가 선행 되어야하며, 보안위험분석은 요구되는 정보보호서비스의 취약점을 해결하고 위협으로부터 시스템을 안전하게 관리할 수 있는 최선의 방법이다.

본 논문에서는 최적의 평가계획을 수립할 수 있는 평가사례기반추론 기능을 모델링하였다. 평가 사례기반추론(case-based reasoning)기능은 보안위험분석평가를 프로젝트단위로 관리하며, 기존의 평가사례 간 유사도를 평가하고, 유사한 평가 사례를 바탕으로 최적의 보안위험분석평가 계획을 수립할 수 있다.

키워드 : 위험분석, 평가사례기반추론

Abstract Information society is dramatically developing in the various areas of finance, trade, medical service, energy, and education using information system. Evaluation for risk analysis should be done before security management for information system and security risk analysis is the best method to safely prevent it from occurrence, solving weaknesses of information security service.

In this paper, Modeling it did the evaluation-base CBD function it will be able to establish the evaluation plan of optimum. Evaluation-based CBD(case-based reasoning) functions manages a security risk analysis evaluation at project unit. it evaluate the evaluation instance for beginning of history degree of existing. It seeks the evaluation instance which is similar and Result security risk analysis evaluation of optimum about under using planning.

Key words : Risk Analysis, Evaluation Case-Based Reasoning

1. 서 론

정보시스템에 대한 정보보안 위험을 인식하면서 정보보안관리 측면의 중요성이 강조되고 있다. 정보시스템에 대한 보안관리는 보안위험분석평가가 선행 되어야하며, 보안위험분석은 요구되는 정보보호서비스의 취약점을 해결하고 위협으로부터 시스템을 안전하게 관리할 수 있는 최선의 방법이다[1]. 대부분의 위험분석평가[2-4]는 수개월 이상의 분석평가 기간과, 다수의 전문평가자가 참여하는 프로젝트 수준의 규모이며, 대상기관의 규모에 따라 방대한 양의 평가결과를 갖게 된다. 따라서 위험분석평가는 쉽지 않은 평가계획, 적지 않은 평가비용, 수개월의 평가기간, 평가 참여인원, 방대한 양의 평가결과로 인한 관리가 필요하며, 최적의 평가계획의 설계가 필요하다.

이러한 배경에서 본 논문에서는 평가사례기반 추론을 이용하여 사례의 재사용 및 사례적용과정 제시를 통한 위험분석 평가에 최적을 평가 프로젝트의 설계를 수립하고 특히 사례 표현하기 위하여 기능요구(보안요구사항), 평가단계, 세부평가(자산평가, 위협평가, 취약성평가, 보안대책) 상호간의 연관 관계를 모델링[5]하였으며, 사례의 기능요구(보안요구사항), 평가단계, 세부평가 간의 연관관계를 이용하여 사례 재사용을 위한 사례적용과정을 제시하였다. 또한 복잡한 평가 프로젝트이나 새로운 평가대상기관의 의뢰가 있을 경우 평가계획에 대한 최적화된 설계를 통한 성공적인 평가계획을 수립할 수 있다. 위험분석 평가에 대한 성능관점에서는 평가에 대한 관리, 평가자의 평가행동에 대한 가이드, 평가기간 단축으로 인한 비용절감, 적정 평가자의 선택을 통한 평가일력을 최적으로 활용할 수 있다.

본 논문의 2장에서는 보안위험분석평가에 적용된 사

· 본 연구는 산업자원부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음
† 정 회 원 : 한국과학기술정보연구원 바이오인포매틱스팀 연구원
bangyh@kisti.re.kr
†† 종신회원 : 한남대학교 컴퓨터공학과 교수
gslee@eve.hannam.ac.kr
논문접수 : 2006년 5월 29일
심사완료 : 2007년 4월 23일

례기반추론[6]과정을 보이고 3장에서는 연관 관계를 모델링 하였다. 4장에서는 평가기간, 평가비용, 조직규모에 대한 성능평가결과를 보이고, 5장에서 끝으로 결론을 맺는다. 본 결과는 위험분석을 수행하는 초기단계 및 진행단계에서 기존의 평가결과를 추론규칙을 통해서 제공받음으로써 위험분석 평가프로젝트 수행에 대한 가이드를 제시하고, 평가기간 및 적정평가자 선정을 통해 체계적인 평가프로젝트를 성공적으로 이룰 수 있을 것이다.

2. 평가 사례기반추론 과정 및 추론 규칙

2.1 평가 사례기반추론 과정

평가 사례기반추론은 위험분석 계획단계에서 기존의 평가결과를 검색규칙을 통해서 가장 검색규칙 값에 가까운 평가결과를 검색한다. 검색된 평가결과는 평가기간, 적정 평가자수, 보안점검분야, 평가결과를 사전에 예측 할 수 있다. 그림 1은 보안위험분석 평가에 적용한 평가사례기반 수행 과정이다.

보안위험분석평가에 적용한 평가사례기반추론은 대상조직의 파악을 통한 사례기반 DB로부터 규칙 값에 가장 근접한 유사사례를 확인하고, 근사 값이 존재하지 않으며 그 외의 값 중에서 근사치가 높은 것을 검색결과로 사용한다. 위험분석에 대한 평가가 종료하면, 평가결과에 대한 기존사례기반과 분석사례를 비교하여 분석사례의 변형을 위해서 도출과 검증을 통해서 새로운 사례로 저장하였다.

평가사례기반추론기능 및 처리에 대한 설명은 다음과 같다.

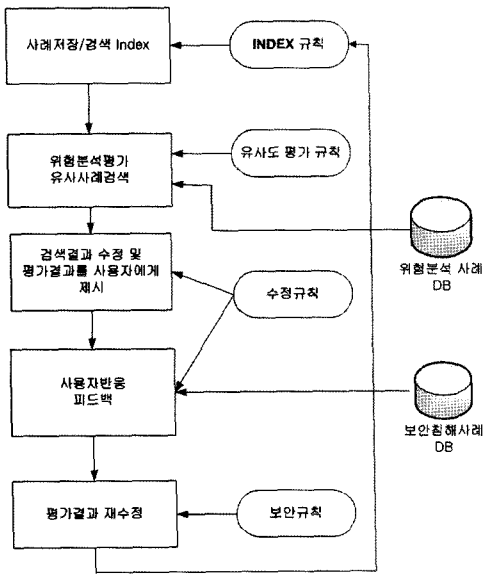


그림 1 사례기반추론 처리과정

① 사용자로부터 특정조직에 대한 속성정보를 입력받으며, 입력받은 속성정보를 위험분석 대상이 되는 입력사례로 간주한다.

② 저장되어 있는 기존의 평가결과 사례 중에서, 상기 입력사례(Case)와 가장 유사도가 높은 위험분석 사례를 검색한다.

③ 검색된 가장 유사한 위험분석 사례에 대한 평가 결과를 이용하여 입력사례에 대해 정보보안수준, 평가기간, 평가자수, 핵심 업무 및 시스템, 자산 가치, 위협수준, 취약점 수준, 보안대책 적용리스트, 위험도 등을 사전에 파악 할 수 있다.

④ 평가결과를 종합하여 상기 특정 조직에 대한 위험을 분석하고, 상기 정보보안 위험 분석 결과를 평가자에게 제공함으로써 평가프로젝트의 성공률을 높일 수 있다.

2.2 추론규칙

평가사례기반추론을 위해서는 추론 규칙이 필요하며, 추론 규칙은 평가결과 검색 또는 평가 결과를 저장할 때 이용된다. 추론규칙은 대상조직의 규모, 보안수준평가결과, 보안수준 인식정도 등을 규칙별 점수로 계산하고 가장 유사한 값을 검색 결과로 사용한다.

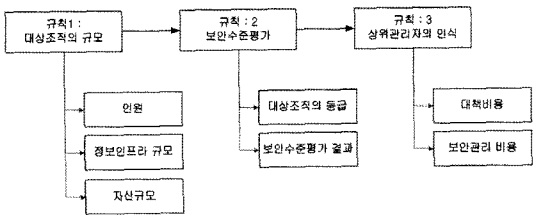


그림 2 추론규칙

3. 평가계획에 대한 문제기술 및 모델정의

3.1 문제 기술

보안위험분석평가는 일련의 평가프로세스를 통하여 최종평가결과를 정략적으로 제시하고, 이에 대한 보안대책을 적용할 수 있어야 한다. 기존에 평가된 평가결과는 새로운 대상기관의 평가에 중요한 정보를 제공한다. 사례기반추론프로세스는 다음과 같은 4단계 과정을 거쳐 이루어진다.

- 평가 계획 : 대상기관의 기관정보로부터 핵심 업무를 파악하여 정보시스템을 분류하고, 자산을 조립선 그래프로부터 보안요구사항을 유도한다.
- 평가구성설계 : 평가구성설계는 각 단계에 대한 평가절차를 설계한다. 설계된 절차는 평가단계(assembly mechanism)라 하며, 평가단계는 각 평가를 담당할 수 있는 평가자, 평가기간, 평가결과에 대한 예정평가시간을 포함한다.

- 평가단계 설계 : 설계된 일련의 평가단계를 배치하고, 세부평가 설계 대안을 생성한다.
- 분석평가 : 시뮬레이션을 통하여 평가단계 설계 대안을 평가한다. 설계대안의 성능이 원하는 값 이상일 경우 그 설계 대안을 선택하고, 그렇지 못한 경우 단계 평가단계 설계, 분석평가를 반복한다.

보안위험분석의 첫째 단계는 평가요구사항을 표현하는 자산 조립선 그래프로부터 평가절차를 유도하였다. 정보시스템에 대한 자산의 위치구조는 조립선 그래프로 표현되며, 평가단계 구조도는 AND/OR 그래프를 이용하여 표현할 수 있다. 일반적으로 조립선 그래프는 자산을 의미하는 노드와 자산 사이의 조립관계를 표현하는 아크로 구성되어 있으며, 아래 그림 3은 자산 a, b, c, d, g 5개로 이루어진 정보시스템의 간단한 조립선 그래프의 예를 도시한다.

$$\begin{array}{l} c-b-g \\ \quad | \\ d-a \end{array}$$

그림 3 조립선 그래프(예)

정보시스템의 자산 조립선 그래프를 평가단계 구조도로 변환하기 위하여 모든 가능한 평가단계를 AND/OR 그래프에 표현한 조립공정도로 변환하여야 한다. 그림 4(a)의 트리구조는 평가단계를 표현하는 예이다.

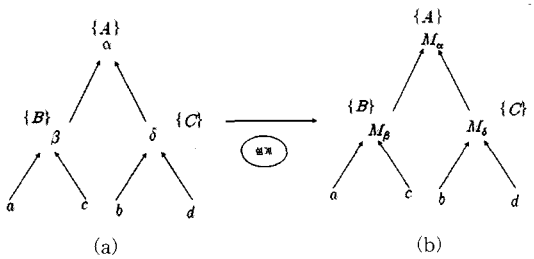


그림 4 평가 설계 조립선 그래프

이 평가단계는 평가방법을 표현하는 노드 $\alpha, \beta, \delta, \ldots$와 정보시스템의 구성자산의 관계를 표현한 아크로 이루어져 있으며, 단말노드 $a, b, c, \ldots$는 최종 자산을 의미한다. 예를 들어 노드 α는 자산 a, b가 α 평가방법에 의하여 평가되어 정보시스템 {A}를 평가하는 것을 표현하고 있다. 평가함수 F_α는 입력자산 리스트 (a,b) 정보시스템 $\{IS\}$로 변환함을 의미하고 T 는 평가의 기술적 제약이라고 정의하자. 그러면 그림 4(a)의 모든 평가는 아래 식 (1)과 같이 표현될 수 있다.

$$F_\alpha(a,b) = \{IS\}, \forall \alpha \in T. \quad (1)$$

식 (1)의 평가함수 , 입력자산리스트, 정보시스템은 평가를 설계하기 위한 보안요구가 된다. 본 논문에서 평가설계를 유도된 평가방법 α에 대한 수행할 수 있는 세부평가 M_α을 생성하는 것이 라고 정의한다. 식 (1)에 의하여 주어진 평가 함수식은 평가수행을 설계하기 위한 보안기능요구이다 . 따라서 평가 설계는 세부평가방법에 따라서, 자산평가 A와 위협평가 T, 취약성평가 V 및 가상평가결과모델 CV 등을 포함한다. 평가 설계는 평가함수 F_α를 입력으로 필요한 세부평가 $M_\alpha = A_\alpha, T_\alpha, V_\alpha, CV_\alpha$를 유도하는 변환 공정으로 간주될 수 있으며, 다음 식 (2)에 의하여 정의된다.

$$\text{평가계획 설계: } F_\alpha \rightarrow M_\alpha, \forall \alpha \in T. \quad (2)$$

3.2 평가 CBR 설계 모델정의

사례기반추론이란 주어진 문제를 해결하기 위해 과거 사례를 검색하여 유사한 사례를 선택하고, 그 해법을 수정 및 보완하여 주어진 문제에 대한 해를 찾는 인공지능의 한 분야이다. 사례기반추론의 문제해결 과정은 그림 5와 같이 크게 사례검색과 사례재사용 과정으로 나누어진다. 사례검색 과정은 다시 유사사례 선택과 선택된 유사사례를 수정하여 초기 해를 제시하는 단계로 분해 될 수 있다. 사례재사용은 사례수정과 사례평가 단계를 통하여 이루어진다.

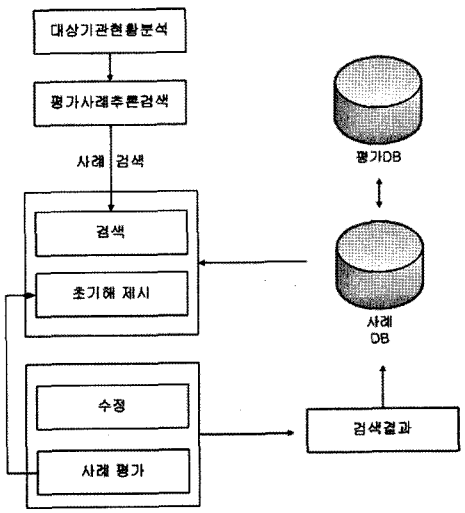


그림 5 사례기반추론 단계

사례기반추론에서는 다음과 같은 점을 고려해야 한다.

첫째, 사례는 과거의 문제풀이 기억을 저장하고 있는 지식으로 간주될 수 있다. 따라서 사례에는 기본적으로 사례가 발생한 상태를 설명하는 문제와 그 문제를 풀기 위해 사용되었던 해답 등을 포함하고 있어야 한다.

둘째, 과거에 경험했던 유사한 사례들 중 현재의 문제와 가장 유사한 사례를 가장 빠른 시간에 찾기 위해서는 과거의 사례를 어떻게 인덱스(index)할 것인가 하는 부분이다.

셋째, 인덱스 한 항목과 더불어 효율적인 사례 검색 방법을 지원하기 위해서는 사례베이스를 어떻게 구성할 것인가 하는 부분이다.

넷째, 사례 검색 과정에서 과거의 사례와 새로운 문제가 얼마나 유사한 지를 어떻게 평가할 것인가 하는 부분이다. 마지막으로 재사용 단계에서 검색된 사례가 현재의 문제와 충분히 유사하지 않을 때에는 검색된 사례에 저장된 해결 방법을 새로운 문제 상태에 맞게 어떻게 수정할 것인가 하는 부분이다.

4. 평가 사례기반추론 모델링

4.1 평가 사례표현

사례 C_i는 평가 설계에 대한 보안 기능적 요구F_i, 그 평가를 수행하는 세부평가단계도 B_i, 세부평가 M_i으로 이루어진 계층구조로 구성된다.

$$C_i = \{F_i,\ B_i,\ M_i\}. \tag{3}$$

보안 기능적 요구 F_i는 평가를 설계하기 위하여 요구되는 평가방법 α_i , 자산 리스트 l_i, 자산수준 리스트 O_i와 기술적 제약요인 T_i로 구성되어 있다. 보안기능요구는 사례 검색을 위한 열쇠가 될 수 있으며, 사례 중에서 문제를 기술하는 부분에 해당된다.

$$\text{보안 기능요구 -> } F_i=\{\alpha_i\ ,\ l_i,\ O_i,\ T_i\}, \tag{4}$$

- α_i = 자산평가방법
- l_i = 자산리스트
- O_i = 자산수준리스트
- T_i = 기술적 제약요인

세부평가 M_i는 평가 설계의 결과로 설계된 M_α = 자산평가 A_α, 위협평가T_α, 취약성평가 V_α, 가상평가결과모델 CV_α 구성된다.

$$M_i = \{A_i,\ T_i,\ V_i,\ CV_i\ \} \tag{5}$$

세부평가의 행위는 세부평가도로 표현될 수 있다. 세부평가는 단위 평가를 정점으로 단위평가 간에 연결 관계를 간선으로 표현한 방향성 그래프이다. 정점에 간선이 연결되는 방법은 아래 그림 4와 같이 (a)정점과 정점 사이를 화살표로 연결하여 순서관계 만을 표현한 경우, (b)정점에 연결된 간선을 모두 거쳐야 하는 AND 관계 그리고 (c) 정점에 연결된 간선 중 1개만 거쳐야 하는 OR 관계의 세 가지로 표현된다고 하자. 예컨대, A라는 자산과 B라는 자산의 연관관계를 갖는 경우도 있고, A라는 자산 B, C와 모두에 종속되어 있는 경우 또는 A라는 자산에 B 또는 C가 종속되거나 종속되지 않는 경우가 존재한다고 볼 수 있다.

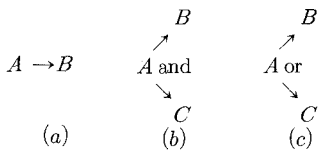


그림 6 세부평가 간 연결 관계

세부평가 간 연결관계는 선.후행 평가 짝으로 표현되며, predicate and와 or를 이용하여 표현 될 수 있다. 그림 6(a, b, c)의 세 가지 연결 관계에 대한 표현은 각각 다음과 같다.

- <A, B>
- <A, and(B,C)>
- <A, or(B, C)>

따라서 세부평가단계도 B_i는 단위평가 집합 u_i, 단위평가 간 연결 관계 집합 r_i의 집합으로 정의될 수 있으며, 다음과 같이 표현된다.

$$\text{세부평가단계도 } B_i = \{u_i,\ r_i\}, \tag{6}$$

- $u_i = \{u_{ij} | \forall j = 1...\text{단위평가수}\}$,
- $r_i = \{r_{ij} | \forall j = 1...reation\ \text{수}\}$.

세부평가 u_{ij}는 다시 세부평가구분 δ_{ij}, 자산 리스트 Ul_{ij}, 자산수준 리스트UO_{ij}, 평가시간 t_{ij}, 평가에 대한 기술적 제약요인 MT_{ij}, 위협평가 T_{ij}, 취약성평가 V_{ij}, 해당 가상평가결과모델 CVS_{ij}로 구성되어 있으며 다음과 같이 표현된다.

$$u_{ij} = \{\delta_{ij},\ Ul_{ij},\ UO_{ij},\ t_{ij},\ MT_{ij},\ T_{ij},\ V_{ij}\ \} \tag{7}$$

이때 모든 단위평가에 대한 자산평가, 위협평가, 취약성평가를 포함하며 다음 식 (8)과 같이, 모든 단위평가에 대한 해당 자산수준의 합은 정보시스템을 의미하며 다음 식 (9)와 같이, 단위평가에 대한 해당 가상평가 모델의 합은 가상평가모델과 같으며 다음 식 (10)과 같이 각각 표현될 수 있다.

$$A \cup T \cup V = \cup MT_i. \tag{8}$$

$$IS = \cup O_i S_i. \tag{9}$$

$$V = \cup VS_i. \tag{10}$$

4.2 유사사례 선택

설계가 요구되는 새로운 평가 설계의 보안기능요구가 주어지면 사례기반으로부터 가장 유사한 사례를 찾는 것은 매우 중요하다. 앞서 언급한 바와 같이 평가의 세부평가도로 표현된다.

유사사례를 선택하기 위하여 두 평가간의 유사정도를 나타내는 평가유사도를 다음과 같이 정의한다. 즉 두 공정설계 기능요구 F_i, F_j 간에 평가유사도 δ_{ij}는 자산의 유사도 δ_{pij}와 단위평가유사도 δ_{wij}의 곱으로 표현될 수 있으며, 자산유사도 δ_{pij}는 두 평가함수 간에 동일한 자산을 공유하고 있는 비율을, 단위평가유사도 δ_{wij}는 두 평가함수 간에 공유하고 있는 단위평가의 비율을 각각 의미하며 다음 식 (11~13)에 표현되어 있다.

$$\delta_{ij} = \delta_{pij} \cdot \delta_{wij} \tag{11}$$

$$\delta_{pij} = \frac{(I_i \cap I_j) + \varepsilon (I_i \cap I_j)^T}{(I_i \cup I_j)} \tag{12}$$

$$\delta_{wij} = S(\alpha_i, \alpha_j) \frac{(v_i \cap v_j)}{(v_i \cup v_j)} \tag{13}$$

- δ_{ij} : 두 평가i, j 간의 평가유사도
- δ_{pij} : 두 평가 i, j 간의 자산유사도
- δ_{wij} : 두 평가 i, j 간의 단위평가유사도
- ε : 가중치.
- $S(\alpha_i, \alpha_j)$: 평가α_i와 α_j의 유사가중치
- $(v_i \cup v_j)$: 평가 i, j 간 상이한 자산 수.
- $(v_i \cap v_j)$: 평가 i, j 간 동일한 자산 수.
- $(I_i \cap I_j)^T$: 평가 i, j 간 기술적 제약요인은 동일, 자산의 분류ID가 상이한 자산 수

구체적인 사례선택 알고리즘은 다음과 같다.

```
Case Retrievel
  input : 새로운 평가project F_n = {α_n, I_n, O_n, T_n};
  output : select case C_s = {F_n, B_s, M_s};
  begin
    for each case IN Case Base
      새로운 평가 대상기관 정보와 유사도를 계산.
      최대 유사도를 갖는 평가사례를 선택.
      선택된 평가case는 C_s = {F_n, B_s, M_s};
      평가사례 F를 선택된 F_s에 대체하고
      F_s를 저장한다.
end
```

4.3 초기해 제시

선택된 사례가 주어진 문제와 동일한 경우 선택된 사례는 문제에 대한 해이다. 그렇지 않은 경우 선택된 사례로부터 초기 해를 작성하여야 한다. 초기 해는 문제의 보안기능요구와 선택된 보안기능요구 사이의 상이한 점을 해소하는 방향으로 이루어진다.

```
SolutionProposal
  input : C_s and F_s;
  output : Proposed case C_p = {F, B_p, M_p};
  begin
    IF(I_n = I_s), C_s는 최종 solution
    for each part p_i IN I_n
      for each part p_j IN I_s
        if 동일자산ID는 처리하지않는다.
        if 동일형, M_s의 parameter 수정
        if I_s에만포함, B_s와 M_s관련노드 제거
        if I_n에만포함, B_s와 M_s에 관련노드 제거
        if I_s에만포함, B_s와 M_s에 관련노드추가
    T_n와 T_s를 비교하여 B_s와 M_s를 수정한다.
  End
```

4.4 사례수정

사례선택과정에서 제시된 평가결과는 과거에 주어진 문제와 가장 비슷한 평가 계획 설계를 이용하여 세부평가의 차이를 수정한해이다. 본 논문의 사례기반추론엔진은 3개의 규칙의 DB 테이블을 수정한다.

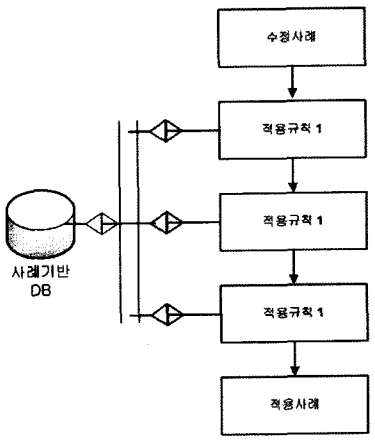


그림 7 사례수정과정

4. 성능평가

성능평가는 보안위험분석 평가계획부터 보안대책 선정 및 적용까지의 기간 동안을 기존분석방법과 사례기반추론을 적용한 방법을 통한 성능평가를 실시하였다. 기존의 평가에 대비 평가기간 및 평가자의 적절한 선택

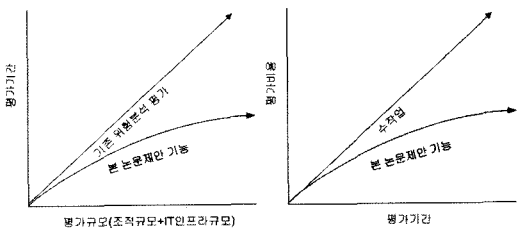


그림 8 평가규모 및 평가기간에 대한 성능그래프

으로 평가비용의 감소를 가질 수 있으며, 초기 사례기반 추론에 대한 평가결과가 존재하지 않기 때문에 평가에 대한 참조데이타의 증가됨으로 본 결과보다 성능이 향상될 것으로 기대된다(본 성능 평가결과는 지식기반 위험분석도구의 프로토타입의 기능의 일부인 평가기반 CBR모델을 적용한 시스템을 대상으로 일부 연구원을 팀으로 나누어 실험한 결과임).

5. 결 론

본 논문에서는 보안위험분석평가를 프로젝트단위로 관리하며, 최적의 평가계획을 수립할 수 있는 평가사례기반추론 기능을 모델링하였다. 평가 사례기반추론(case-based reasoning) 기능은 기존의 평가사례 간 유사도를 평가하여 유사한 평가이웃사례를 찾아내고, 평가이웃사례의 결과를 이용하여 최적의 보안위험분석평가 계획 수립할 수 있다.

본 결과는 위험분석을 수행하는 초기단계 및 진행단계에서 기존의 평가결과를 추론규칙을 통해서 제공받음으로써 위험분석 평가프로젝트 수행에 대한 가이드를 제시하고, 평가기간 및 적정평가자 선정, 보안대책비용의 추정 등을 통해 체계적인 평가프로젝트를 성공적으로 이룰 수 있을 것이다.

향후, 평가기간의 단축을 위해서, 인공지능을 이용한 대책선정, 실시간 위험분석을 위한 모델링, 프로젝트 스케줄링관리에 대한 연구가 이루어 져야 할 것이다. 또한 도구의 개발을 완벽히 하고 현장에서 적용시험이 필요할 것이다.

참 고 문 헌

[1] Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim, "Security Risk Analysis Model for Information Systems," LNCS 3398, Systems Modeling and Simulation: Theory and Applications: Third Asian Simulation.

[2] Young-Hwan Bang, YoonJung Jung, Injung Kim, Namhoon Lee, GangSoo Lee, "The Design and Development for Risk Analysis Automatic Tool," ICCSA2004, LNCS 3043, pp. 491-499, 2004.

[3] OCTAVE, "OCATVE Criteria, Version 2.0," Carnegie Mellon Software Engineering Institute(2001. 12), OCATVE Method Implementation Guide Version 2.0, OCTAVE, 2001. 6, http://www.sei.cmu.edu/publications/pubweb.html.

[4] CSE, "A Guide to Security Risk Management for IT Systems," Government of Canada, Communications Security Establishment(CSE)," 1996.

[5] A. Finkelstein et al. (ed.), "Software Process Modeling and Technology," John Wiley&Sons, 1994.

[6] Ellis Horowitz, Sartaj Sahni, Fundamentals of Computer Algorithms, Computer Science Press Inc. Computer Software Engineering Series, pp. 198-200.

[7] SSE-CMM, "Project, Systems Security Engineering Capability Maturity Model (SSE-CMM) - Model Description Document," V.2, http://www.sse-cmm.org, 1999. 4. 1.

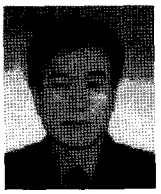
[8] ISO/IEC 14598-1, "IT-Software product evaluation, Part 1. General overview," 1997. 3.

[9] FIPS-191, "Specifications for Guideline for The Analysis Local Area Network Security," NIST, Nov. 1994.

[10] OCTAVE, "OCATVE Criteria, Version 2.0," Carnegie Mellon Software Engineering Institute(2001. 12), OCATVE Method Implementation Guide Version 2.0, OCTAVE, 2001. 6, http://www.sei.cmu.edu/publications/ pubweb.html.

방 영 환

1997년 한남대학교 컴퓨터공학과(학사) 2002년 대전대학교 대학원 컴퓨터공학과(석사). 2002년~2005년 대전보건대학 컴퓨터정보처리과 프로그래밍 전문강사. 2006년 한남대학교 대학원 컴퓨터공학과 박사. 2007년~현재 한국과학기술정보연구원 바이오인포매틱스 팀. 관심분야는 보안공학, 위험분석평가, 바이오인포매틱스



이 강 수

1981년 홍익대학교 전자계산학과 학사 1983년 서울대학교 대학원 전산학과(석사). 1989년 서울대학교 대학원 전산학과(박사). 1985년~1987년 국립한밭대학교 전자계산학과 전임강사. 1992년~1993년 미국일리노이대학교 객원교수. 1995년 한국전자통신연구원 초빙연구원. 1998년~1999년 한남대학교 멀티미디어학부장. 1987년~현재 한남대학교 컴퓨터공학과 정교수. 관심분야는 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼