효과적인 위협관리를 위한 보안 위험도 평가기법

(Security Risk Evaluation Scheme for Effective Threat Management)

강 필 용 †

(Pilyong Kang)

요 약 중요 IT 자산에 대한 보안성 강화를 위해서는 관련 위협(또는 취약점)의 식별 및 이에 대한 보안 대비책의 적정성 분석이 선행되어야 한다. 이를 위해 본 논문에서는 자산 및 위협에 기반한 보안 위험도 평가기법을 제안한다. 제안한 기법은 식별된 자산 및 위협 관련 공격시도 탐지와 취약점 점검 등의 대응 범위 및 수준의 사전 점검과 정량적인 위험도 평가를 제공함으로써 기존 연구에 비해 효과적으로 위협관리 업무에 활용될 것으로 기대된다.

키워드 : 위협관리, 위험평가

Abstract It is most important that identifying security threats(or vulnerabilities) of critical IT assets and checking the propriety of related security countermeasures in advance for enhancing security level. In this paper, we present a new security risk evaluation scheme based on critical assets and threats for this. The presented scheme provides the coverage and propriety of the countermeasures(e.g., intrusion detection rules and vulnerability scan rules, etc.), and the quantitative risk level of identified assets and threats. So, it is expected that the presented scheme will be utilized in threat management process efficiently compared to previous works.

Key words : Threat Management, Risk Evaluation

1. 서 론

인터넷 웜·바이러스 유포, 해킹 등 최근의 인터넷·컴퓨터 보안 위협 및 관련 침해사고는 날로 발생 주기가 짧아지고 있음은 물론, 지능화 및 복잡화됨으로써 적절한 대응이 매우 어려워지고 있다. 이에 따라 보안 관리자는 최신 보안 위협 및 취약점을 사전에 파악하고, 관련 보안장비의 설치·구성 등 보안관리 운영환경 전반에 대한 점검 및 대응책을 마련해야 하는 등 전문지식이 요구되고 있다.

이에 대한 대응으로 최근, 위협관리시스템이 주목받고 있다. 이는 전사적인 IT 자산에 대한 위협 및 보안 정보의 수집·분석과 경보·관리를 지원하는 통합 보안관리 시스템으로 정의할 수 있다. 특히, 로컬 영역에서의 침입 탐지, 트래픽 분석 및 상관관계 분석 등의 위협분석 외에도, 공신력 있는 외부 정보보호기관으로부터의 최신 위협 정보들을 수집 및 분석하여 보안 관리자에게 제공함으로써 취약점의 사전 점검 등 침해사고 대응체계를 구축함으로써 체계적인 보안성 향상을 도모할 수 있다[1,2].

보안 관리자 입장에서는 무엇보다 중요 자산에 대한 공격시도 탐지규칙 및 취약점 점검규칙 등 현재의 보안관리 체계가 적절히 적용 및 운영되고 있는지 판단하는 것이 필수적이지만, 현실은 여의치 못한 실정이다. 즉, 기존의 연구 및 제품들은 보안 로그에 대한 분석 등 제한된 정보만 제공할뿐, 운용중인 보안체계가 중요 자산에 영향을 줄 수 있는 공격을 얼마나 탐지할 수 있는지, 운용중인 보안 취약점 스캐너가 해당 위협을 얼마나 커

· 이 논문은 제34회 추계학술대회에서 '효과적인 위협관리를 위한 보안 위험도 평가기법'의 제목으로 발표된 논문을 확장한 것임

† 정 회 원 : 한국인터넷진흥원 정보보호본부
kangpy@kisa.or.kr

논문접수 : 2008년 1월 16일
심사완료 : 2009년 5월 25일

정보과학회논문지: 시스템 및 이론 제36권 제5호(2009.10)

버하는지 여부 등 총체적인 대응 수준에 대한 점검을 지원하기엔 미흡하다.

이에 본 논문에서는 중요 자산 및 위협(또는 취약점) 별 보안 위험도 평가기법을 제안함으로써, 식별된 보안 위협에 대한 대응체계의 적정성 점검 및 정량적인 위험도 평가를 통한 우선순위 부여 등 효과적인 위협관리를 지원하고자 한다.

본 논문의 구성을 살펴보면, 2장에서는 기존 연구 및 제품을 살펴봄으로써 장·단점 분석 및 개선방안을 모색한다. 3장에서는 위협관리 오픈 프레임워크에 기반한 시스템 모델 및 위험도 평가기법을 제안하고, 4장에서는 제안한 기법의 구현 및 분석 예제를 통해 가능성을 확인하고, 주요 고려사항 및 향후 연구과제를 제시한다. 마지막으로 5장에서는 결론을 맺는다.

2. 관련 연구

본 장에서는 기존의 위협관리시스템 및 위험평가방법론을 살펴보고, 문제점 및 개선방안을 제시한다.

2.1 위협관리시스템

본 절에서는 대표적인 위협관리시스템 중 하나인 시스코의 Threat Response(TR)[3]과 시만텍의 DeepSight Threat Management System(TMS)[4]를 중심으로 관련 동향을 살펴본다.

시스코 TR은 보안 위협에 대한 대응을 지원하는 시스템으로, 공격시도 탐지로 인해 발생한 침입경보에 대해 관련 노드에 설치된 운영체제 및 취약점 점검결과를 참조한 검증을 지원한다. 즉, 엔터프라이즈급 네트워크 환경에서 발생하는 수많은 침입경보에 대한 필터링을 제공함으로써, 실제 공격에 대해 보다 효과적이고 신속한 대응을 지원할 수 있다는 장점을 제공한다. 그러나, 탐지규칙 및 취약점 점검 환경이 알려진 위협에 대비하여 얼마나 충분히 준비되어 있는지는 사전에 알 수 없고, 관련 취약점 점검결과가 누락된 경우엔 운영 효과가 많이 떨어지는 단점이 있다.

최근 국내외에서 많이 사용되고 있는 시만텍 DeepSight TMS는 네트워크 현황 및 글로벌 취약점 정보 제공을 비롯하여 로컬 사이트의 보안 이벤트 관리, 취약점 점검 등 위협관리를 지원한다. 이를 통해 보안 관리자는 보호 대상 사이트 관리는 물론, 글로벌 위협 정보에 기반해서 관리 대상의 안전성을 사전에 점검 및 대비함으로써 보안성을 강화할 수 있다. 그러나, 공격시도 탐지규칙 및 취약점 점검규칙 등 운용중인 보안체계의 적정성 여부에 대한 체계적인 분석은 지원하지 않는다.

2.2 위험평가방법론

위험(risk)이란 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성으로 정의할 수 있다[5-7]. 손실 및 위험의 수준을 표현하는 방법에 따라 크게 정량적인 방법과 정성적인 방법으로 구분될 수 있으며, 평가된 위험의 규모에 따라 수용할 위험과 수용할 수 없는 위험을 분류하고 수용할 수 없는 위험에 대해서는 위험 규모에 따라 우선순위에 따른 적절한 대응책을 마련해야 한다.

위험의 유형과 규모를 확인하기 위해서는 위험에 관련된 모든 요소들과 그들이 어떻게 위험의 규모에 영향을 미치는 지를 분석해야 한다. 일반적으로 IT 환경에서의 위험은 자산, 위협, 취약성의 함수로 정의될 수 있으며, 다음은 연간 예상 손실액을 기준으로 대표적인 위험평가 계산식을 나타낸 것이다.

$$\text{연간 예상 손실}(A, T) = \text{자산 } A\text{의 가치} \times \text{위협 } T\text{의 연간 발생횟수} \times T\text{에 대한 A의 취약성} \quad (1)$$

위험평가방법론 및 이를 지원하는 자동화 도구는 수없이 많으며, 최근엔 침입시도 탐지정보 및 취약점 점검결과 등을 실시간으로 활용한 동적인 평가를 지원하는 시도가 주목을 받고 있다. 이러한 동적인 환경에서 보다 정확한 평가를 위해서는 최신 위협에 대한 침입시도 탐지규칙[1] 및 취약점 점검규칙[2] 등에 대한 적정성 분석이 필요하지만, 기존 연구에서는 이에 대한 지원을 찾아보기 어렵다. 즉, 보안 대응체계에 대한 총체적인 분석을 지원하는 위험도 평가체계가 요구된다.

2.3 기존 연구 및 제품의 문제점

앞에서 살펴본 것처럼 기존 연구 및 제품은 중요 자산별 침입경보와 자산 정보 및 취약점 점검결과 등을 참조한 실제 공격여부 검증과 위험도 계산을 통한 우선순위 부여 등 위협 대응 업무를 수행하지만, 사전에 탐지규칙 및 점검규칙의 범위와 적정성 등의 사전 점검을 지원하기엔 미흡하다. 특히, 가장 중요하다고 볼 수 있는 위협관리의 적정성 여부를 사전에 판단하기엔 많은 어려움이 있다.

요컨대, 효과적인 위협관리를 위해서는 공격 탐지규칙 및 취약점 점검규칙 등 보안장비 구성의 적정성 점검 등에 기반한 총체적인 위험도 측정을 통한 우선순위 도출 및 대응책 수립이 필요하다.

3. 자산 및 위협 기반 위험도 평가기법

본 장에서는 효과적인 위협관리를 위한 보안 위험도 점검절차 및 정량적인 위험도 평가기법을 제시한다.

---

1) 과거의 감사자료로부터 공격에 이르는 특정한 패턴을 정의한 규칙(Rule). 예컨대, 비인가된 접속시도 등 공격시도 과정에서 송·수신되는 네트워크 패킷들에 대한 특정한 패턴을 기반으로 침입시도를 탐지할 수 있음

2) 보호 대상 자산에 대한 취약점 존재여부를 점검하기 위한 규칙. 예컨대, 특정 보안패치의 설치여부나 특정 포트의 개방여부 등이 점검규칙이 될 수 있음

3.1 위협관리 모델

본 논문에서 고려하는 위협관리 모델은 침입경보 및 취약점 점검결과 등 다양한 보안 로그를 수집, 알려진 위협(또는 취약점) 및 중요 자산과의 상관관계 분석을 통해 보안 대응책의 누락여부 체크 및 정량적인 위험도를 계산하고, 우선순위 부여를 통한 적절한 대응을 지원한다.

그림 1은 전형적인 위협관리 절차를 나타낸 것으로 각 구성 요소를 살펴보면, 다양한 보안장비로부터의 보안로그 및 이벤트 수집, 정규화, 상관관계 분석, 위험도 계산 등으로 구성된다.

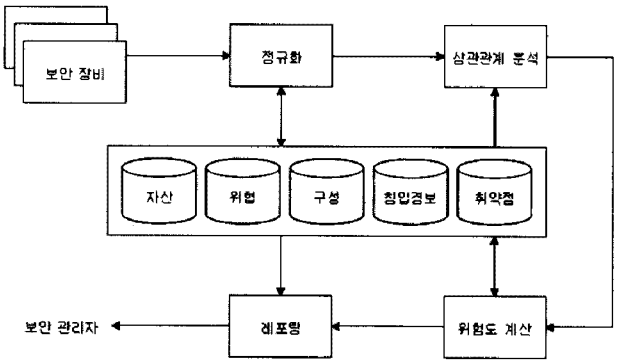

그림 1 전형적인 위협관리 절차

일반적으로 모든 환경에 최적인 단일 보안 시스템은 존재하지 않으므로, 다양한 보안 모듈을 적절하게 연동 및 통합할 수 있는 운영환경을 구축하는 것이 바람직하다. 이에 본 논문에서는 다양한 보안 장비로부터의 보안 로그를 수집하고, 이들간 상관분석 등을 지원하는 위협관리 오픈 프레임워크[8]의 활용을 제안한다. 그림 2는 이에 대한 구성의 예를 나타낸 것으로, 각 모듈은 통신 허브를 통한 에이전트간 메시지 전달기법에 기반하여 연동한다.

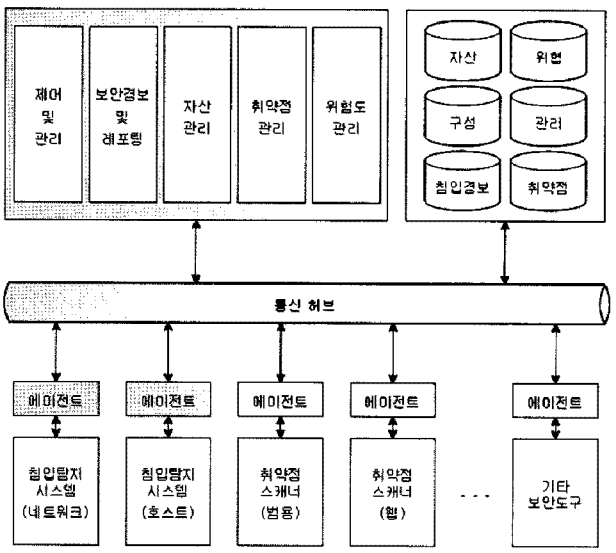

그림 2 위협관리 오픈 프레임워크

이러한 환경에서 각 보안 모듈은 에이전트에 기반한 연동을 통해 보안 어플리케이션의 소스코드 변경없이 손쉽게 연동될 수 있다. 즉, 실시간 통신 기반과 표준 인터페이스, 데이터베이스, 제어 및 조회 화면 등 공통의 관리 기능이 제공됨으로써 개발자는 통신 기반에 대한 지식이 없어도 손쉽게 통합 운영환경을 구현할 수 있다. 이러한 프레임워크와 관련된 사항은 본 논문의 범위를 벗어나므로 자세히 언급하지 않는다.

3.2 보안 위험도 점검

본 절에서는 중요 자산 및 알려진 위협에 대한 위험도와 탐지규칙 및 점검규칙 등의 적정성을 점검하기 위한 절차와 이에 따른 점검표 작성을 제안한다. 그림 3은 구체적인 점검절차를 나타낸 것으로, 단순히 식별된 취약점만을 나열하거나 자산과 취약점 및 공격시도 탐지정보 간의 연관성 만을 점검하는 기존 연구와는 다르게 자산 및 위협과 관련된 보안도구의 대응여부 등을 점검표를 이용해 점검함으로써 보안 대책의 준비여부를 손쉽게 확인할 수 있는 장점을 제공한다.

참고로 본 논문의 예제에서는 문제를 단순화하기 위해 침입탐지시스템과 취약점 스캐너만을 기준으로 점검을 수행하지만, 침입차단시스템 등 관련 보안장비가 더 있는 경우엔 해당 점검절차를 3-2단계 이후에 계속 추가할 수 있다.

보안 관리자는 작성된 보안 점검표를 통해 최신 위협에 대응한 공격시도 탐지규칙 또는 취약점 점검규칙 등의 누락여부를 사전에 점검함으로써 관련 보안도구의 구성을 보완할 수 있다. 이에 대한 자세한 사항은 본 논문의 4장에서 간단한 예제를 통해 살펴본다.

3.3 보안 위험도 평가

본 논문에서는 자산 및 위협별 정량적인 위험도 계산을 위해, 자산별로 탐지된 공격시도, 취약점, 충격도, 자산가치를 기반으로 총체적인 위험수준을 산출함으로써 우선순위 부여 및 지속적인 관리를 지원하는 체계를 제안한다.

표 1은 위험도 평가를 위한 계산식에 사용되는 함수를 정의한 것으로, 자산에 대한 색인($0 \leq i \leq n-1$) 및 위협에 대한 색인($0 \leq t \leq m-1$)을 사용한다.

$T(i)$가 반환하는 공격시도 정도는 관리자가 정의한 일정시간 동안 수집된 침입경보에 대해 자산 및 취약점 정보를 참조하여 실제 공격시도로 검증된 값이다. 예컨대, 자산 i가 갖는 취약점에 대한 최근 일주일 동안의 시간당 평균 공격횟수 등으로 표현될 수 있다.

$I(t)$가 반환하는 충격도는 취약점 t의 취약도를 나타내는 것으로 값이 클수록 자산에 미치는 영향이 크며,

1단계 : 새로운 보안 위협/취약점 수집 (즉, 위협 데이터베이스를 갱신)

2단계 : 보호 대상에 관련 자산이 있는지 점검 (즉, 위협과 자산을 매핑)

3단계 : 자산 관련 위협에 대응한 보안장비(도구) 구성을 점검

3-1 : 관련 공격시도 탐지규칙 적용여부 점검, 규칙을 운용하는 경우 탐지 횟수 조사
(즉, 자산 관련 위협에 대한 침입탐지시스템의 탐지여부 및 빈도 확인)

3-2 : 관련 취약점 점검규칙 적용여부 점검, 규칙을 운용하는 경우 취약점 발견 여부 조사
(즉, 자산 관련 위협에 대한 취약점 스캔 지원여부 및 스캔 결과 확인)

4단계 : 보안 점검표 작성을 통해 누락된 취약점, 탐지규칙, 점검규칙 등 추가
(즉, 보안 대응체계 보완)

5단계 : 정량적인 위험도 및 대응도 계산

그림 3 보안 위험도 점검절차

표 1 위험도 계산을 위한 함수 정의

함수	내용
$T(i)$	자산 i에 대한 검증된 공격시도 정도를 반환
$T(i, t)$	취약점 t를 갖는 자산 i에 대한 검증된 공격시도 정도를 반환
$I(t)$	위협(취약점) t에 대한 충격도(취약도)를 반환
$V(i)$	자산 i가 갖는 취약점 색인 리스트를 반환
$A(i)$	자산 i에 대한 가치(관리자 부여)를 반환
$A(i, t)$	취약점 t를 갖는 자산 i에 대한 가치를 반환
$P_A(j, t)$	보안도구 유형 j의 위협 t에 대한 대응여부(0 또는 1)를 반환

일반적으로 3단계 또는 5단계의 값이 많이 사용되고 있다.

본 논문에서는 일반적인 접근과 유사하게 자산 및 위협별 위험도를 공격도(T), 충격도(I), 자산가치(A)의 곱으로 표현한다. 자산 i에 대한 위험도, $R_A(i)$는 다음의 식 (2)에 의해 계산되며, $\sum I(V(i))$는 자산 i가 갖는 모든 취약점에 대한 충격도의 합으로 계산된다.

$$R_A(i) = T(i) \times \sum I(V(i)) \times A(i) \quad (2)$$

위협 t에 대한 위험도, $R_T(t)$는 다음의 식 (3)에 의해 계산될 수 있다. 즉, 위협 t와 관련된 모든 자산에 대한 공격도 및 자산가치와 충격도의 곱으로 그 크기를 정량적으로 표현한다.

$$R_T(t) = \sum_{i=0}^{n-1} T(i,t) \times I(t) \times \sum_{j=0}^{n-1} A(j,t) \quad (3)$$

위협 t를 이용한 공격에 대한 대응도, $P_T(t)$는 다음의 식 (4)에 의해 계산될 수 있다. k는 보안도구 유형의 수를 나타낸다. 예컨대, 침입탐지시스템과 취약점 스캐너가 설치되어 각각이 위협 t에 대한 대응책을 지원하면 1, 둘 중 하나만 지원하면 0.5, 하나도 지원하지 않으면 0이다.

$$P_T(t) = \frac{\sum_{j=0}^{k-1} P_T(j,t)}{k} \quad (4)$$

자산 i의 위협 및 공격에 대한 대응도, $P_A(i)$는 다음의 식 (5)에 의해 계산될 수 있다. $COUNT(V(i))$는 자산 i가 갖는 실제 취약점의 수를 반환하며, $\sum P_T(V(i))$는 자산 i가 갖는 취약점별 대응도의 합으로 계산된다. 즉, $0 \le P_A(i) \le 1$이며, 식별된 모든 취약점에 대한 대응책이 존재하면 1이다.

$$P_A(i) = \frac{\sum P_T(V(i))}{COUNT(V(i))} \quad (5)$$

본 논문에서 제안한 공격시도, 취약점 및 충격도, 자산가치는 모두 정성적 및 정량적 평가가 가능하며, 관리자 부여 가중치를 제공하면 운영환경에 맞게 계산식을 보정할 수 있다. 무엇보다 기존의 연구에서는 제공하지 못한 자산 및 취약점별 총체적인 대응도를 정량적으로 표현할 수 있다는 장점을 제공한다.

4. 구현 및 분석

본 장에서는 제안한 기법의 가능성 분석을 위해 간단한 구현 사례를 중심으로 분석결과를 살펴본다.

4.1 시험 구현 및 운영환경

본 논문에서는 그림 4와 같이 침입차단시스템 및 침입탐지시스템, 취약점 스캐너 등이 설치된 일반적인 보안 환경을 예제로 선택하였다.

위협 데이터베이스는 CVE(Common Vulnerabilities Exposures)[3][9], 네트워크 기반 침입탐지시스템(NIDS-

3) 다양한 보안도구간 원활한 취약점 공유를 위한 것으로 '09년 6월 현재, 36,795개가 등록되어 있으며, 40개 조직 및 기관에서 75개의 제품 및 서비스가 공식적으로 호환성을 제공하고 있음

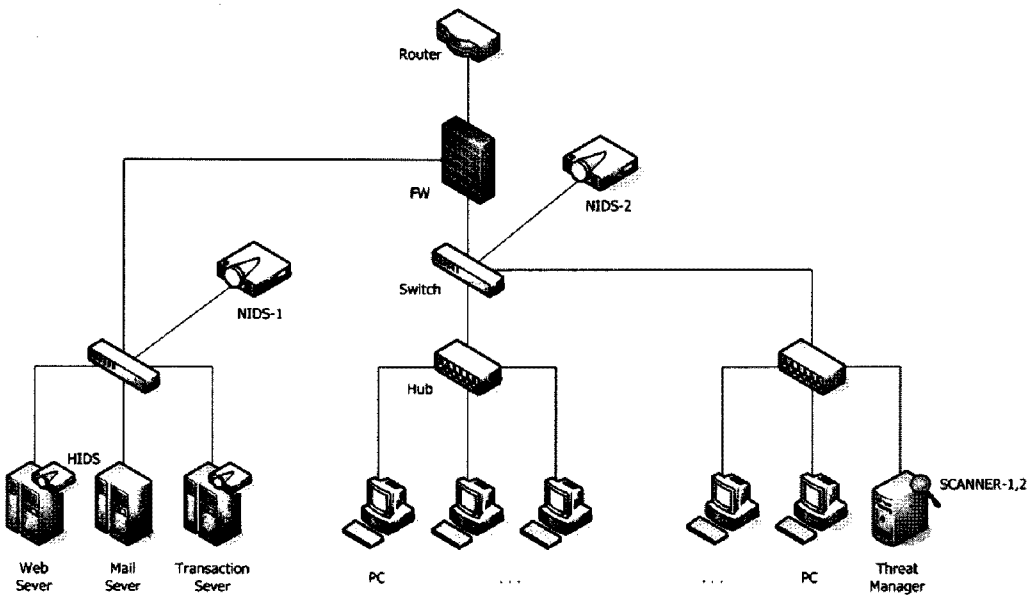

그림 4 시험 운영환경

1,2)은 SNORT[10], 호스트 기반 침입탐지시스템(HIDS)은 A사의 제품, 취약점 스캐너(SCANNER-1,2)는 NESSUS[11] 및 SARA[12]를 활용하고, 자산관리 모듈은 자체적으로 구현함으로써 시험 운영환경을 구축하였다.

4.2 보안 점검표 작성

그림 5는 시험 운영환경에서 제안한 보안 위험도 점검절차에 따라 보안 점검표를 작성한 예제를 나타낸 것이다.

점검표에서 '×' 표시는 관련 사항의 누락 또는 보안도구의 미설치, '√' 표시는 관련 사항의 존재 또는 보안도구의 설치를 의미하며, ( )에는 침입탐지시스템의 공격시도 탐지횟수 및 취약점 스캐너의 취약점 점검결과를 함께 표시함으로써 공격빈도 및 취약여부를 함께 판단할 수 있다.

예컨대, 본 점검표를 통해 관리자는 위협 1과 관련된 자산을 비롯하여 관련 침입탐지시스템 및 취약점 스캐너가 운영환경에 설치되어 있으며, 최근 위협 1 및 자산과 연관이 있는 취약점의 존재 및 공격시도가 있었음을 한눈에 파악할 수 있다.

이러한 보안 점검표를 기반으로 관리자가 수행해야할 대응 업무를 대표적인 사례별로 살펴보면 다음의 표 2와 같다. 사례 ①은 위협이 부재한 경우로 관련 탐지 및 점검 규칙을 참조한 신규 위협의 추가가 요구되며, 사례 ③ 및 ④는 각각 침입탐지시스템의 탐지 규칙 및 취약

구분 \ 위협/취약점	1	2	3	4	5	6	①×
자산(OS, SW) 관련	√	√	√	√	√	②×	√
NIDS-1 탐지규칙	√(0)	√(5)	③×	√(0)	√(3)	√(0)	√(9)
NIDS-2 탐지규칙	√(10)	√(13)	×	√(0)	√(0)	√(0)	√(21)
HIDS 탐지규칙	×	√(3)	×	√(1)	×	√(0)	×
SCANNER-1 점검규칙	√(O)	√(-)	√(×)	×	×	④×	√(O)
SCANNER-2 점검규칙	√(O)	√(O)	×	√(×)	√(-)	×	×

※ 기호는 각각 발견(O), 미발견(×), 미점검(-)을, ( )의 숫자는 탐지 횟수를 의미

그림 5 보안 위험도 점검 예제

표 2 점검표 기반 위협관리 예제

사례	상태	행동
①	관련 위협 부재	위협 데이터베이스엔 없으나, 관련 자산과 탐지 및 점검 규칙이 존재하면 신규 위협 정보를 자체적으로 추가
②	관련 자산 부재	관련 자산이 존재하지 않으므로 관련 탐지 및 점검 규칙을 적용할 필요가 없음
③	관련 침입탐지 규칙 부재	관련 탐지규칙을 제공하지 않는 경우, 해당 탐지규칙을 자체적으로 생성(또는 개발업체에 요청)하거나 이를 지원하는 침입탐지시스템을 설치
④	관련 취약점 점검규칙 부재	관련 점검규칙을 제공하지 않는 경우, 해당 점검규칙을 자체적으로 생성(또는 개발업체에 요청)하거나 이를 지원하는 취약점 스캐너 설치

점 스캐너의 점검 규칙이 부재한 경우로 관련 위협 정보를 참조한 신규 규칙의 추가가 요구됨을 알 수 있다.

이처럼 점검표 작성은 중요 자산과 관련된 취약점의 사전조사와 공격시도의 탐지 및 대응체계를 종합적으로 진단해볼 수 있는 장점을 제공한다. 또한, 시스템 구축을 통한 자동 점검시 해당 자산 및 취약점에 대해서만 점검을 수행함으로써 점검 효율을 향상시킬 수 있다.

요컨대, 제안하는 기법을 활용하면, 알려진 위협에 대한 보안 미비사항을 사전에 정확하게 파악함으로써 시의적절한 대응을 통한 보안 수준의 향상을 기대할 수 있다.

4.3 위험도 평가 및 시각화

그림 6은 시험 운영환경에서 최신 위협(취약점) 10개에 대한 위험평가 결과를 시각화한 예제를 나타낸 것이다. 자산 및 위협, 보안도구별로 다양한 시각화가 가능한데, 본 예제에서는 최신 위협과 관련된 자산의 가치, 보안도구별 대응도 및 보안 이벤트 발생 정도를 함께 나타냄으로써 운영환경에 대한 직관적인 인지를 지원함을 알 수 있다. 예를 들어, 보안 관리자는 위협별 위험도 산출을 통해 위협 2, 6번에 대한 즉각적인 취약점 제거 및 보안도구 설치 등 보호대책 수립의 우선순위 등을 도출할 수 있다.

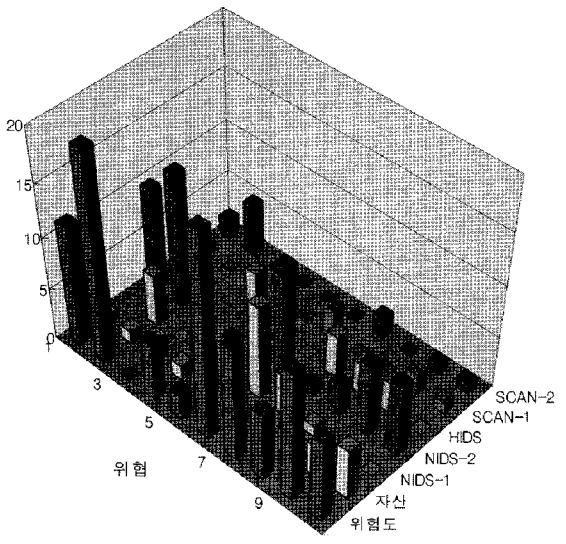

그림 6 위협별 위험도 및 대응수준 시각화 예제

이처럼 제안한 기법을 적용하면, 식별된 최신의 위협에 대한 동적인 위험도를 효과적으로 시각화함으로써 단순히 취약점의 나열에 그친 기존의 정적인 충격도(피해도)에 제한된 분석이 아닌, 운영환경이 반영된 시의적절한 대응체계를 구축할 수 있는 장점을 제공할 수 있을 것으로 기대된다.

4.4 중요 고려사항 및 향후 연구과제

제안한 기법의 효과적인 구현을 위해서는 위협 및 취약점, 침입탐지 규칙, 취약점 점검규칙 등에 대한 공통의 식별자가 필요하다. 현재, 관련 연구로는 CVE가 있으나, 이에 대한 상호운용성을 지원하는 보안도구인 경우에도 모든 취약점에 대해 100%의 상호연동을 보장하는 것은 아니므로 많은 추가 작업이 요구된다. 즉, 아직도 대부분의 보안도구들이 많은 수의 자체 취약점을 제공하고 있다. 또한, CVE가 알려진 모든 취약점을 포함할 수 없으므로 실제 운영환경에서는 BugTraq[13] 등과 같은 새로운 위협의 추가 및 수정 등 편집 기능도 요구된다.

요컨대, 효과적인 운영을 위해서는 무엇보다 보안도구들이 관련 위협에 대한 연결고리(즉, 공통의 식별자)를 제공함으로써 대응여부의 검색이 용이해야 한다. 향후 공통의 식별자를 100% 지원하는 제품이 연동되면 효과가 배가될 것으로 기대되며, 점진적으로 그러한 환경으로 변화할 것으로 예상된다.

한편, 실제 운영환경에서는 중요 자산에 대해 알려진 모든 취약점을 점검하는 것보다는 최신 또는 중요 취약점에 대해서만 점검하는 것이 보다 효율적이다. 즉, 주기적으로 최신 및 중요 취약점에 대한 우선적인 점검 및 관리가 바람직하다.

5. 결 론

본 논문에서는 중요 자산(네트워크 및 호스트 등)에 대한 위협관리의 적정성 및 위험도를 사전에 검증하기 위해 중요 자산 및 알려진 위협에 대한 위험도 평가기법을 제안했다. 제안한 기법은 식별된 위협에 대응한 보안관리 체계가 공격시도 탐지 및 취약점 점검 등을 통해 얼마나 대비하고 있는지 정량화된 분석결과를 제공

함으로써, 총체적인 보안 대응 수준을 보안 관리자가 사전에 점검 및 판단할 수 있도록 지원한다. 요컨대, 본 연구결과는 중요 자산을 위협하는 알려진 보안 위협에 대한 사전 점검을 강화하고, 우선순위 부여를 통한 적절한 대응을 유도함으로써 보호 대상의 보안성 향상에 기여할 것으로 기대된다.

참 고 문 헌

[1] S. Drew, "Reducing Enterprise Risk with Effective Threat Management," *Information Systems Security*, vol.13, Jan. 2005, pp.37-42.
[2] S. J. Scott, "Threat Management Systems - The State of Intrusion Detection," Snort Documents, Aug. 2002, http://www.snort.org/docs/threatmanagement.pdf
[3] Cisco Threat Response, http://www.cisco.com
[4] Symantec DeepSight Threat Management System, http://www.symantec.com
[5] G. Stonebumer, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems," *NIST SP 800-30*, NIST, July 2002.
[6] British Standard Institute, "Guide to BS7799 Risk Assessment," *PD 3002:2002*, 2002.
[7] ISO/IEC JCT 1/SC 27, "Guidelines for the Management of IT Security(GMITS) - Part 3: Techniques for the Management of IT Security," *ISO/IEC TR 13335-3:1998*, 1998.
[8] P. Kang and W. Sim, "Message-based Open Framework for Security Incidents Prevention and Response," *Proceedings of the JWIS 2007*, Japan (Tokyo), Aug. 2007, pp.395-408.
[9] CVE - Common Vulnerabilities and Exposures, MITRE, http://www.cve.mitre.org
[10] SNORT - The Open Source Network Intrusion Detection System, http://www.snort.org
[11] NESSUS - Vulnerability Scanner, http://www.nessus.org
[12] SARA - Security Auditor's Research Assistant, http://www-arc.com/sara/
[13] BUGtraq, http://www.securityfocus.com

강 필 용

1996년 숭실대학교 컴퓨터학부(공학사)
1998년 숭실대학교 컴퓨터학과(공학석사)
2001년 숭실대학교 컴퓨터학과(공학박사)
2001~현재, 한국인터넷진흥원 수석연구원. 관심분야는 시스템 및 네트워크 보안, 보안성 평가