情報保護學會論文誌
第14券 第2號, 2004. 4

ISP(Internet Service Provider) 네트워크의 정량적인 위험분석을 위한 시스템 설계 및 구현

문 호 건[a)†‡], 최 진 기[a)], 김 형 순[b)]
KT 기술연구소[a)], 부산대학교[b)]

Design and Implementation of Quantitative Risk Analysis System for ISP Network

Ho-Kun Moon[a)†‡], Jin-Gi Choe[a)], Hyung-Soon Kim[b)]
Technology Laboratory KT[a)], Pusan National University[b)]

요 약

ISP 네트워크의 보안수준 진단과 대응방안을 수립하기 위해서는 네트워크상의 정보자산에 대한 취약점과 위협 요인을 식별하고, 피해 발생시 예상되는 손실의 정도를 산정하는 위험분석 절차가 필수적이다. 하지만, 기존의 위험분석 방법론 및 도구들은 대부분 방법론적 분석절차와 수단만을 제공하며, 개별 시스템의 취약점 및 위협요인의 변동정보를 실시간으로 반영할 수가 없다. 따라서, 본 논문에서는 네트워크 침입탐지 시스템과 취약점 분석 시스템의 탐지 정보들을 실시간으로 수집, 분석하여 네트워크 자산에 발생할 수 있는 위험의 가능성을 찾아내고, 정량적인 위험수준을 평가하는 시스템을 제안한다. 또한, 실험을 통해 시스템의 성능수준을 제시하였다.

ABSTRACT

Risk analysis process, which identifies vulnerabilities and threat causes of network assets and evaluates expected loss when some of network assets are damaged, is essential for diagnosing ISP network security levels and response planning. However, most existing risk analysis systems provide only methodological analysis procedures, and they can not reflect continually changing vulnerabilities and threats information of individual network system on real time. For this reason, this paper suggests new system design methodology which shows a scheme to collects and analyzes data from network intrusion detection system and vulnerability analysis system and estimate quantitative risk levels. Additionally, experimental performance of proposed system is shown.

Keywords: *Risk, Quantitative Analysis, Asset Value*

Ⅰ. 서 론

오늘날 대부분의 ISP(Internet Service Provider)들은 네트워크를 통해 연결된 수많은 정보자산들을 각종 사이버 공격으로부터 효과적으로 방어하기 위해 다양한 대응 수단을 도입, 운용하고 있다. 이때, 대응 방안과 수준을 결정하는 수단으로 네트워

접수일: 2004년 2월 17일; 채택일: 2004년 4월 7일
† 주저자, ‡ 교신저자 : hkmoon@kt.co.kr

크 자산(Asset)의 취약점(Vulnerability)과 위협(Threat)요인에 대한 정보를 이용하는 위험분석 방법론(Risk Analysis Methodology)을 사용한다. 그러나, 대부분의 위험분석 방법론[1-7]과 도구(Tool)[8-10]들은 보안시스템의 도입을 위한 컨설팅 또는 정기적인 보안진단을 위해 사용되며, 위험분석을 위한 정형화된 분석절차와 수단을 제공하는 것이 대부분이다. 이 같은 위험분석 방식으로는 ISP 네트워크에서 임의 시점에 사이버 공격으로 인해 발생 가능한 위험의 원인과 예상 손실수준(Impact)을 신속, 정확하게 파악하기가 어렵다.

첫째, 네트워크 자산이 지닌 취약점과 위협요인은 수시로 변동할 수 있기 때문에 특정 시점에서 분석한 네트워크의 위험수준은 결코 현재의 위험수준을 정확히 반영하고 있다고 할 수 없다.

둘째, 네트워크 자산에 위험을 일으키는 각종 취약점과 위협을 탐지하기 위해 취약점 분석 시스템(Vulnerability Analysis System, 이하 VAS)과 네트워크 침입탐지 시스템(Network Intrusion Detection System, 이하 N-IDS)을 주로 운용하고 있다. 그러나, 이들 시스템들이 제공하는 대량의 탐지정보들 간에 존재하는 연관성들을 분석하고, 가공하는 작업은 전적으로 보안 관리자의 수작업에 의존하고 있어 보안사고의 가능성과 영향을 신속하고, 효과적으로 분석할 수가 없다.

셋째, 기존의 위험분석 방법론과 도구들은 위험을 자산, 취약점 및 위협수준의 통합적 속성으로 보고 이들의 조합에 의해 위험수준을 정하고 있다. 그러나, 정량적인 값으로 표현되는 자산가치와 정성적인 형태로 표현되는 취약점 및 위협수준을 조합할 경우, 위험수준의 설정 단계수가 많아지고, 위험수준을 정량적으로 제시하기 어려워 결과의 객관성이 저하되는 문제가 있다.

넷째, 대부분의 위험분석 방법론과 도구들은 ISP가 현실적으로 관리하기 힘든 다수의 정성적인 척도(Metric)들을 사용하고 있어 시스템으로 구현하기가 어렵다.

따라서, 자산에 발생할 수 있는 위험에 효과적으로 대응하기 위해서는 위험발생 요인의 변화를 지속적으로 측정, 관리하고, 위험발생에 따른 예상 손실수준을 실시간에 가깝게 정량적으로 평가할 수 있는 새로운 방법이 필요하다. 이를 위해 본 논문에서는 우선 네트워크에서 운용하는 상용 N-IDS 및 VAS의 탐지정보들을 상호 연동하여 특정자산에 직접적인 위험을 유발할 수 있는 위협과 취약점의 연관성(Correlation)을 찾아낼 수 있는 방법을 이용하였다. 또한, ISP 네트워크가 생성하는 서비스의 가치를 이용하여 개별 자산의 가치와 예상손실 수준을 추정할 수 있는 방법과 연계함으로써 네트워크의 위험수준을 정량적으로 나타낼 수 있는 시스템을 구현하고 설계방법과 실험결과를 제시하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구동향에 대해 소개하고, 3장에서는 본 논문에서 사용한 자산의 정량적 위험수준 산정 방법을 간략히 서술한다. 4장에서는 제안하는 시스템의 구조를 제시하고, 기능 구성 및 분석 알고리즘에 대해 설명한다. 5장에서는 네트워크 상에서 실험한 결과를 보이며, 마지막으로 결론과 향후 연구방향을 제시한다.

II. 관련연구

현재 대부분의 위험분석 방법론 및 도구들은 위험분석을 위한 척도와 기준이 지나치게 세분화되어 있어 복잡하고 다양하게 구성된 네트워크와 조직의 자산들을 다루기 위해서는 많은 전문 인력과 시간이 필요하다. 이 같은 문제로 인해 네트워크의 위험수준을 지속적으로 관찰하고 대응해야 하는 보안관리자에게는 자동화된 위험분석 시스템의 도입이 필요하다. 그러나, 현재 취약점 및 위협요인의 변동정보를 실시간으로 반영하여 위험수준을 정량적으로 평가할 수 있는 시스템은 없다.

따라서, ISP 네트워크의 정량적 위험분석 시스템과 관련된 기존의 연구는 위험파악(Risk Identification)을 위한 부분과 위험평가(Risk Assessment)를 위한 부분으로 나누어 살펴볼 필요가 있다.

2.1. 위험파악 관련 연구

네트워크에 위험을 일으키는 요인은 다양하게 정의할 수 있으나 시스템의 기술적 취약점과 사이버 상의 위협으로 제한하여 고려한다. 네트워크에 대한 각종 위협의 발생을 탐지하고, 예상되는 위험의 유형과 발생 가능성을 정확히 분석하기 위한 기존의 연구는 다음과 같이 분류할 수 있다.

1) 침입탐지 정보의 연관성 분석 기법

N-IDS의 탐지정보들 간에 내재된 연관성을 분석

하여 경보 오류(False Positive)를 줄이고, 네트워크 상의 위협을 효과적으로 탐지하기 위한 연구들이 활발하다. 이러한 시도들은 N-IDS 엔진 자체에 새로운 기술을 적용함으로써 문제를 해결하려는 접근방식으로 다음과 같이 5가지 범주로 나눌 수 있다.[11-15]

- Data Mining Approach
- Rule-based Approach
- Situation-aware Approach
- Probabilistic Approach
- Prioritizing Approach

상기의 접근 방식은 적용에 따른 성능상의 한계 및 관련 데이터 생성의 어려움이 여전히 남아있다 .

2) 취약점과 위협정보의 연관성 분석 기법

이 방법은 네트워크에서 VAS를 통해 사전에 탐지한 취약점 정보와 N-IDS의 위협탐지 정보들 간의 데이터 연관성 분석기법을 이용하여 경보 오류를 줄이고, 네트워크 자산이 지닌 취약점에 대한 위협만을 선별하며 제공한다.[16-18] 따라서, 불필요한 탐지정보를 확인, 분석하는데 따른 운용상의 부담을 크게 줄여줄 수 있지만, 현실적으로 탐지되는 위협의 대부분을 차지하는 네트워크 공격-Scanning, DoS성 공격 등-에 대해서는 적용할 수 없다는 단점이 있다.

3) 시스템 로그(Log)의 연관성 분석 기법

ESM(Enterprise Security Management)을 이용하여 네트워크 상에서 운용되는 다양한 장비들로부터 발생하는 로그 데이터들 간의 인과관계를 분석하는 방법에 대한 연구가 활발하다. 탐지된 위협과 대상 시스템의 로그정보를 함께 수집하여 연관성을 분석함으로써 위험발생 가능성을 정확히 탐지하고, 관리 시스템에 경보를 전달하여 신속한 대응조치를 하는 것을 목표로 하고 있다. 이 같은 기능을 지원하기 위해서는 네트워크상의 주요 관리대상 시스템들에 위협을 탐지할 수 있는 센서기능을 갖는 에이전트(Agent)를 두어야 하고, 서로 상이한 형태의 로그 포맷을 통일된 형태로 변환하여 데이터베이스화 하는데 복잡한 과정이 필요하다. 이같은 개념을 구현한 일부 제품[19]들이 출시되고 있으나 정책설정 과정이 복잡하고, 에이전트 설치에 따른 시스템의 기능지원에 제약이 있으며, 네트워크 구성 환경에 따라 시스템 로그들 간의 연관성을 규정하는데 많은 시간이 소요되는 단점이 있다.

2.2 위험평가 관련 연구

위험평가는 자산이 위협에 노출되어 발생할 수 있는 손실의 정도로 나타낼 수 있으며, 기존의 방법론과 도구들이 사용하는 평가 방법은 정량평가와 정성평가로 나눌 수 있다.[20-22]

정량평가는 자산의 가치(Asset Value), 위협의 발생율(Annualized Rate of Occurrence), 노출지수(Exposure Factor) 등을 계량적인 수치로 추정할 수 있다는 가정을 기반으로 하는 평가방법이다. 그러나 위협의 발생율과 자산가치를 추정할 수 있는 데이터의 확보가 어렵다는 문제가 있다. 특히 정보자산의 가용성 상실로 오는 손실을 정량적으로 추정하는 것은 매우 어려운 문제이기 때문에 대규모 정보시스템의 정량적 위험분석은 객관성의 확보에 어려움을 겪고 있다.

정량적 위험평가의 문제를 해결하기 위한 대안으로 서술적인 형태로 표현되는 평가척도를 사용하여 위험을 등급화하는 정성적 위험분석 방법이 이용된다. 정성적 위험분석 방법은 자산, 위협, 취약성 등의 엔티티(Entity)들을 각각의 평가척도에 따라 등급화한 후 이들을 조합하여 위험수준을 산정하는 방법이다. 하지만 정성적 위험분석 방법은 평가자의 주관적 판단에 따라 분석결과가 영향을 받기 때문에 결과의 객관성과 의사결정을 위한 계량적 분석의 결여라는 문제를 지니고 있다.

Ⅲ. 자산가치 및 손실수준 평가 방법

일반적으로 자산이라 함은 조직에 가치를 갖는 모든 것으로 정의되며, 그 분류 기준 및 가치 산정방법도 다양하게 제시되고 있다. 제안하는 시스템에서는 ISP 네트워크의 위험발생에 따른 손실수준을 정량적으로 나타내기 위해 문호건[23]이 제안한 자산손실 모델링 기법을 이용한다. 이 방법을 통해 네트워크상의 특정한 자산이 복수개의 서비스 제공을 통해 생산하는 총 가치(ISP의 경우, 서비스 제공 수입)에서 개별 자산이 기여하는 정도를 정량적으로 추정함으로써 자산의 가치와 예상손실을 간단하고 신속하게 평가할 수 있다.

3.1 네트워크 자산가치 기본 모델

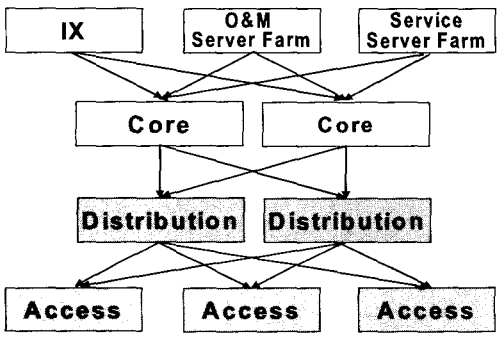
(그림 1)과 같이 계층 구조를 갖는 ISP 네트워크

가 n 개의 물리적인 자산요소로 구성되고 네트워크 자산들의 집합을 A라고 할 경우, 자산집합 A는 수식(1)로 표현할 수 있다.

$$A=\{a_1,\ a_2,\ a_3, \ldots, a_n\} \quad (1)$$

특정 자산 a_k는 구매시점을 기준으로 x 년째의 고정자산 가치를 $Vf(a_k, x)$, 같은 해에 생산한 서비스 가치를 $Vs(a_k, x)$라고 하면 해당 연도에 a_k의 총 가치 $Vt(a_k, x)$는 수식 (2)와 같이 고정자산 가치와 서비스 가치의 합으로 나타낼 수 있다.

$$Vt(a_k, x) = Vf(a_k, x) + Vs(a_k, x) \quad (2)$$



*O&M(Operation and Maintenance)
*IX(Internet eXchange)

그림 1. ISP 네트워크의 구성 모델

자산 a_k의 고정자산 가치 $Vf(a_k, x)$는 매년 가치가 선형적으로 감소하여 통신장비의 일반적인 회계기준인 5년이 지나면 잔존 가치가 0, 또는 Vfr로 수렴하게 된다. 자산 a_k의 서비스 가치 $Vs(a_k, x)$는 ISP 네트워크에서 x 년도에 개별 자산 a_k를 통해 m개의 서비스가 제공될 경우, 하나의 서비스가 생산하는 가치를 $Vpsw(a_k, x)$라고 하면, a_k를 통해 생산되는 총 서비스가치 즉, ISP가 a_k로부터 얻는 서비스 제공 수입은 수식 (3)과 같이 나타낼 수 있다.

$$Vs(a_k, x) = \sum_{h=1}^{m} V_{psw_h}(a_k, x) \quad (3)$$

만일, 특정한 자산의 서비스 가치가 고정자산 가치와 $Vs > 10\,Vf$ 의 관계가 있다면 서비스 가치가 자산의 전체가치의 주된 요소이므로 $Vt \cong Vs$로 근사할 수 있다.

3.2 자산의 서비스 가치 추정 방법

수식 (3)에서 언급한 $V_{psw}(a_k, x)$를 실제의 ISP 네트워크에서 측정하기는 매우 어렵다. 그 이유는 자산이 개별 서비스를 생산하는데 기여하는 정도는 시간에 따라 변화하고, 각 자산이 처리하는 트래픽 중 특정 서비스와 관련된 트래픽을 구분하여 측정하는 것이 거의 불가능하기 때문이다.

네트워크는 개별 자산들의 유기적인 결합을 통해 서비스 가치를 생성하므로, 자산의 서비스 가치를 평가할 때는 네트워크가 생산하는 전체 서비스 가치에서 개별 자산이 가치 생산에 기여하는 정도, 즉 $Vs(a_k, x)$를 역으로 추정하는 방식을 사용하는 것이 현실적이다. 서비스 생산가치의 추정을 위해 개별 서비스의 제공에 이용되는 네트워크 자산요소와 서비스별 연간 생산가치(서비스 매출)를 (표 1)과 같이 정리하면, 연간 총 생산서비스 가치에서 개별 자산이 가치 생산에 기여하는 정도를 추정하는 것이 가능해진다.

표 1. 서버계층 자산의 서비스가치 산출예제

서비스명	서비스 가치 (단위 억)	관련 자산 #1	관련 자산 #2	관련 자산 #3	관련 자산 #4
서비스 0	400	a[0]	a[1]	a[2]	a[3]
서비스 1	200	a[1]	a[2]	a[3]	a[4]
서비스 2	100	a[2]	a[4]		

단, $a[i]$: 서버계층의 i 번째 자산
$Vs[i]$: $a[i]$자산의 서비스가치
$prio[a_k]$: 동일 계층 내에서의 타 자산과 비교한 $a[i]$의 중요도

ISP 네트워크의 설계 및 서비스 특성에 대한 기본 가정[24-25]을 바탕으로, 자산 $a[0] \sim a[4]$들의 서비스 가치를 각각 $V_s[0] \sim V_s[4]$라 하면,

$V_s[0]$ = 400/4 = 100
$V_s[1]$ = 400/4 + 200/4 = 150

$V_s[2] = 400/4 + 200/4 + 100/2 = 200$
$V_s[3] = 400/4 + 200/4 = 150.$
$V_s[4] = 200/4 + 100/2 = 100$

따라서, 동일계층 내 각 자산들의 서비스 가치를 기준으로 한 중요도는 다음과 같은 순위로 된다.

$prio[a_2] \rangle prio[a_1] = prio[a_3] \rangle prio[a_0] = prio[a_4].$

이런 연산 방식은 모든 네트워크 계층에 대해서 공통적으로 적용 가능하며, 이상의 방식을 적용하여 네트워크의 보안 위험이 발생했을 때 침해를 입은 개별 자산들의 손실액을 총자산가치를 기준으로 추정할 수 있다.

3.3 자산의 서비스 가치 손실액 추정 방법

개별 자산의 서비스 생성가치가 허용오차 범위내에서 연간 일정하게 유지된다고 가정하면, 장애발생 자산의 연간 서비스 가치가 10억인 임의 자산 a_k가 보안사고로 인해 장애발생 시점부터 복구시점까지 6시간 동안 서비스를 못했을 경우, 정량적인 예상 서비스 손실액은 수식 (4)로 간단히 추정할 수 있다.

$$V_{Loss}(a_k, x) = Vs/(365*24) * T$$
$$= \{10억/(365*24)\} * 6(시간)$$
$$\simeq 684,931원 \quad (4)$$

위험으로 인해 자산에 발생하는 가치의 손실은 네트워크에서 동일 기능을 수행하는 등가자산의 수와 구성형태에 따라 달라질 수 있다. 등가자산의 일부가 정상적인 서비스 제공을 할 수 없을 때 나머지 등가자산이 서비스를 처리하는 방식에 따라 손실을 계산하는 방식[23,26]이 달라진다.

Ⅳ. 위험분석 시스템 설계

4.1 설계 고려사항

네트워크의 위험발생 요인을 지속적으로 측정, 관리하고, 위험발생에 따른 예상 손실수준을 실시간에 가깝게 정량적으로 평가하기 위해서는 위험분석을 위한 각종 척도들 중 ISP 네트워크에서 측정 및 관리가 가능한 것만을 선택할 필요가 있다. 따라서, 상용 N-IDS와 VAS를 각각 네트워크 상의 위협정보와 자산의 취약점 정보를 수집하는 수단으로 활용하고, 이들 시스템간의 정보연동은 외부 DB에서 수행함으로써 특정 솔루션 벤더의 시스템에 독립적으로 구현 가능하도록 설계하였다. 그 결과, N-IDS 시스템 자체의 자산관련 정책을 별도로 설정, 갱신할 필요가 없이 네트워크로 유입되는 일상적인 유해 패킷의 총량과 네트워크 자산에 직접적으로 영향을 미칠 수 있는 유해 패킷에 관한 분석 정보를 동시에 관리하는 것이 가능하다.

제안하는 위험분석 시스템은 위협의 대상이 되는 자산을 중심으로 이들 위협이 해당 자산에 어떤 위험을 일으킬 수 있는지를 분석하기 위해 탐지정보의 속성 및 시간 정보와의 연관성 해석방식을 개선하였다.

4.2 시스템 구조 및 기능

제안하는 시스템은 (그림 2)와 같이 N-IDS와 VAS의 탐지 정보를 수집하는 모듈(①)과 이들 정보를 이용하여 N-IDS의 로그를 서버에 대한 위협과 네트워크에 대한 위협으로 나누어 분석하는 모듈(②) 및 개별 자산의 가치 및 예상 자산손실 값을 저장하는 DB인 자산관리 모듈(③)로 구성된다. 각 구성 모듈의 기능은 다음과 같다.

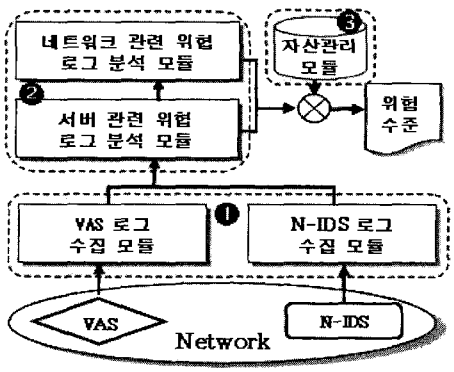


그림 2. 위험분석 시스템 구조도

1) 자산관리 모듈

본 시스템에서는 자산의 정량적인 가치 수준을 미리 산정하여 자산관리 DB에 저장한다. VAS와 N-IDS에서 탐지되는 취약점 및 위협정보에 의해 위

험이 발생하거나 발생이 예상되는 특정 시스템 정보를 자산의 예상손실 수준정보와 연계하여 위험분석을 한다. 자산정보의 속성은 시스템 명, 시스템 운영체제(O.S)명, 네트워크 주소정보(IP), 자산 가치정보, 예상 자산손실 정보 및 기타 관리 정보로 구성되며, (그림 3)과 같은 형태로 자산관리 DB에 저장한다.

2) 로그 수집 모듈

상용 N-IDS와 VAS가 제공하는 위협 및 취약점 탐지정보는 SNMP (Simple Network Management Protocol) Trap으로 데이터를 가져와 외부 DB에 저장한다. 네트워크에 위험을 일으키는 요인은 다양하게 있으나, N-IDS와 VAS로 측정할 수 없는 것은 고려하지 않는다. N-IDS와 VAS의 로그 수집정보 중 위험분석에 필요한 데이터만 선별하여 (그림 3)과 같이 각각 사전 정의한 형태의 DB로 구성한다. 이때, N-IDS와 VAS DB간의 연관성 분석을 위해 IP 어드레스와 CVE(Common Vulnerability and Exposures)-ID[27]를 연관 Key값으로 사용한다.

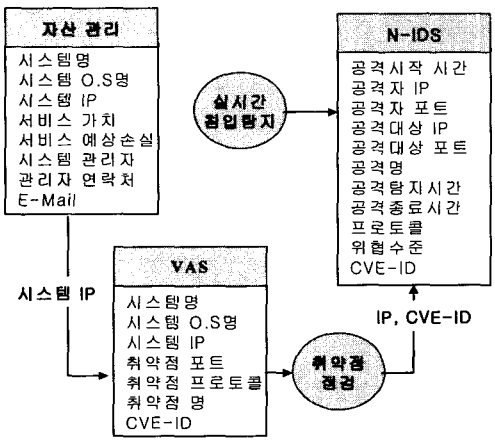


그림 3. 시스템 DB 구성도

3) 로그 분석 모듈

로그 분석 모듈은 기존의 N-IDS 탐지성능 개선을 위한 연구에서 시도한 접근방식과는 달리 N-IDS의 로그를 속성에 따라 서버관련 위협로그와 네트워크관련 위협로그로 분류하여 분석하는 방식을 사용한다. 이때 서버관련 위협로그는 VAS 로그와의 상관분석을 통해 최적화할 수 있다. 네트워크관련 위협로그는 공격의 대상 별로 임의 시간간격 동안 발생하는 위협의 빈도와 연속적으로 나타나는 위협의 형태에 따른 분석을 통해 위험발생 가능성을 나타낼 수 있도록 하였다.

4.3 분석 알고리즘

N-IDS는 서버의 소프트웨어적인 취약점을 찾기 위한 탐색(Scanning), 서버의 각종 취약점에 대한 위협 및 다양한 유형의 비정상적인 징후들에 대한 탐지 로그를 제공한다[28]. 또한, 시간에 따라 네트워크에서 탐지되는 위협의 종류와 위협발생원에 대한 정보를 상세히 알려준다. 그러나, 위협대상 자산의 관점에서 해당 자산에 대해 시간에 따른 위협발생 형태와 그로 인한 위험발생 가능성을 추론할 수 있는 정보를 제공하지는 못하고 있다.

본 연구에서는 이 같은 문제를 해결하기 위해 N-IDS의 로그 정보를 속성에 따라 분리하여 해석하는 방법과 효과적인 정보 표현방식을 제안한다.

1) 서버관련 위협로그 분석

시스템에 내재한 취약점의 존재는 잠재적인 위협을 현실화시킬 수 있는 역할을 하며, 특정한 취약점에 대해 다수의 위협이 상관된다. 취약점을 제거하면 대부분의 서버관련 위협은 네트워크 자산에 실질적인 위험을 일으킬 수 없다.

N-IDS와 VAS의 탐지정보를 상관시키면, 서버의 취약점을 이용하여 위험을 발생시킬 수 있는 위협정보만을 찾아낼 수 있다. 또한, N-IDS의 문제점으로 지적되는 무의미한 오류 경보정보를 줄일 수 있어 운용자의 관리부담을 줄여준다. (그림 4)는 VAS가 탐지한 특정 취약점에 대해 N-IDS의 로그가 상관되는 형태를 보인다.

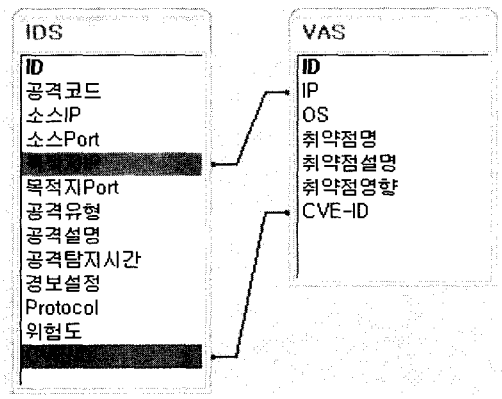


그림 4. VAS와 N-IDS 로그의 상관도

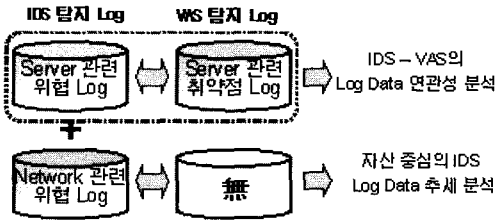


그림 5. VAS와 N-IDS DB의 상관도

그러나, (그림 5)에서와 같이 VAS DB에는 서버의 소프트웨어적인 취약점에 관한 정보만 있어 N-IDS의 로그 중 서버의 취약점에 대한 위협로그만 최적화할 수 있고, 네트워크에 대한 그 밖의 위협은 별도의 해석기법이 필요하다.

2) 네트워크관련 위협로그 분석

N-IDS의 침입탐지 로그중 서버의 취약점에 대한 위협을 제외한 나머지가 네트워크관련 위협로그로 남는다. 기존의 N-IDS는 네트워크에서 탐지된 각종 위협을 단순히 발생순서에 따라 경보 로그를 남김으로써 개별 위협발생원의 공격추이와 위협수준을 파악하기가 어려운 단점이 있다. 또한, 대부분의 위협은 발신원의 주소를 변조하여 이루어지므로, 본 논문에서는 위협을 받고 있는 자산별로 일정 시간동안 발생하는 위협패턴을 하나의 DB 레코드로 관리함으로써 위험발생 가능성이 있는 자산의 식별과 위험 가능성을 효과적으로 인식할 수 있는 방법을 제안한다.

(그림 6)은 네트워크관련 위협로그 분석모듈의 개념도이다. 먼저 N-IDS로부터 순차적으로 수집되는

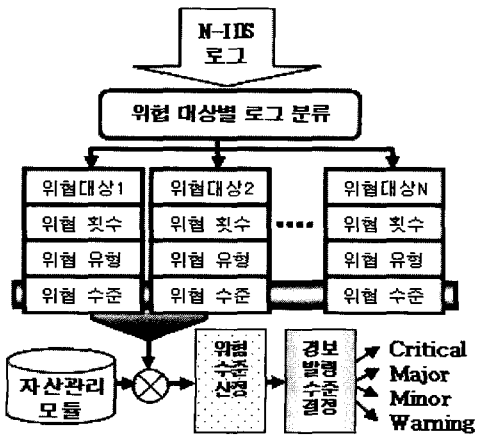


그림 6. 네트워크관련 위협로그 분석 개념도

로그를 위협대상 자산별로 DB레코드를 생성하고, 단위 시간동안 발생하는 위협의 횟수와 유형을 추가해 나간다. 이때 위협유형 정보는 (그림 7)과 같은 형태로 관리되며, 보안관리자가 특정 자산에 대해 시간에 따른 위협의 변화를 용이하게 관찰할 수 있도록 해준다. 특정 자산에 대해 새로운 위협이 발생할 때마다 시간순으로 동일 DB 레코드에 추가하여 기록해 나간다.

[Attack Time, Source IP, Target Port, Attack Name, Protocol, Risk]
[2004/01/05 11:01:00, 1.1.1.2, 137, Netbios Name query, TCP, Low]
[2004/01/05 11:06:10, 1.1.1.3, 53, DNS Reverse Query, UDP, High]
[2004/01/05 11:08:41, 1.1.1.8, 23, Telnet, TCP, Medium]
……

그림 7. 위협유형 관리정보의 내용

3) 위협수준 산정

N-IDS의 위협 DB에는 탐지한 개별 위협의 속성에 따라 사전 설정된 위협수준 정보를 갖고 있다[15]. 따라서, 본 논문에서는 특정 자산에 대한 위협의 빈도와 개별 위협에 대해 N-IDS에서 사전 설정한 위협수준 정보를 이용하여 수식 (5)와 같이 자산에 대한 네트워크 위협의 누적 수준을 산정한다.

$$\text{위협수준} = \sum_{i=1}^{n} T_i \qquad (5)$$

(n : 위협발생 횟수, Ti : i 번째 위협의 수준)

수식 (5)에서 일정 시간간격(Time Window) 동안 산정된 위협수준의 누적 값이 일정치 이상이면 위협대상 자산의 가용성에 문제를 일으킬 수 있는 위협이 지속된다고 판단한다. 이때 위협수준 산정을 위한 시간 간격과 위협수준의 구분은 네트워크의 트래픽 분포, 장치용량 및 서비스의 구성을 고려하여 결정한다.

4) 위험수준 산정 및 경보발령 수준 결정

특정 자산의 취약점에 대한 직접적인 위협이 발생하거나, 반복적으로 발생하는 위협으로 인해 위협수준이 일정수준을 넘을 경우, 자산관리 모듈에서 위협대상 자산들의 서비스 예상 손실액을 위험수준의 산정값으로 제공한다. 그런데, 네트워크 운영측면에서 경보발령 수준의 결정은 위협 대상의 자산가치가 전체 자산가치에서 차지하는 비중과 함께 자산에 대한 위협의 수준을 함께 고려하여 결정한다. 자산의 상대

적 가치가 낮아도 해당 자산의 정상적인 운영에 장애가 발생할 정도의 위협수준이 탐지될 경우에는 그 정도에 따라 신속한 대응이 필요하고, 단위 시간동안 위협의 빈도는 낮아도 상대적으로 높은 가치를 갖는 자산의 경우는 위협의 진행상황을 면밀히 관찰할 필요가 있기 때문이다.

일반적으로 경보 수준은 4단계(Critical, Major, Minor 및 Warning)로 구분하며, 본 시스템에서 각 단계의 구분을 위한 임계값(Threshold) 설정은 단위시간동안 발생한 위협수준의 평균값을 이용하여 설정한다.

경보발령 수준은 (그림 8)과 같은 알고리즘을 이용하여 결정한다. 발생한 공격이 자산이 가지고 있는 잔류 취약점을 직접적으로 공격하는 것이라면 단계가 가장 높은 Critical 경보를 발생시킨다. 네트워크 공격의 경우, 이전 동일시점의 위협수준을 비교하거나 공격 대상 자산이 전체 자산가치에서 차지하는 비중을 고려하여 경보수준을 결정하게 된다. 따라서 자산의 비중이 높고 위협수준이 과거동일 시점보다 일정수준 이상 될 경우에는 Critical 경보를 발생시킨다. 그러나 가치가 상대적으로 낮은 자산에 대한 위협수준이 과거 동일시점보다 큰 경우에는 정도에 따라 Warning, Minor, Major 경보를 발생시킨다.

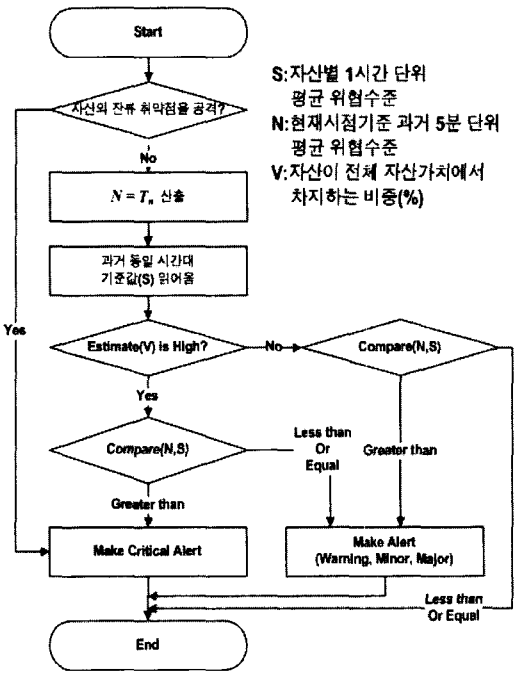


그림 8. 경보발령 수준결정 알고리즘

V. 실험 및 평가결과

5.1 실험환경 및 방법

제안하는 시스템은 7가지 운영체제(O.S)를 사용하는 총 1006 대의 서버들로 구성된 네트워크를 대상으로 실험을 하였다. 실험에는 다음과 같은 장비들로 구현된 시스템을 사용하였다.

- N-IDS : WINS Technet사 Sniper 3.0
- VAS : NileSoft사 SecuGuard NSE 1.2
- DBMS : MS SQL 2000

실험을 위해 서버의 취약점 분석은 3일에 한번씩 모든 시스템을 대상으로 이루어졌으며, N-IDS의 로그는 4일 동안 탐지한 위협정보를 이용하였다.

본 시스템이 제안하는 위협로그 분석 알고리즘을 이용하여 N-IDS에서 반복적으로 탐지되는 동일 로그를 속성에 따라 통합적으로 표현해줌으로써 전체 로그 수를 90%이상 줄일 수 있었다. 또한, 사전 설정한 기준에 의해 특정 자산에 대한 위협이 발생한 경우의 위험수준과 경보수준을 산출한 결과를 보인다.

5.2 실험결과 및 분석

(표 2)는 특정시점에 네트워크를 대상으로 VAS를 이용하여 1006 대의 시스템에 대한 취약점을 분석한 결과로서 총 32 대의 시스템에서 15가지의 취약점이 탐지되었다. (표 3)은 제안한 방법에 따라 4일 동안 발생한 모든 공격에 대해서 위협대상 자산별로 구분하였을 경우, N-IDS 로그가 모두 90%이상 감소함을 보이며, 이는 다수의 위협들이 특정한 자산에 대해서 반복적으로 이루어졌음을 의미한다.

표 2. VAS 점검 결과

Telnet 서비스 실행 취약점	6대
Telnet 서비스 정보제공 문제	5대
Cisco router의 http server 설정 취약점	5대
Daytime 취약	4대
X server 포트 오픈 취약점	2대
ICMP timestamp 요청 취약점 외 기타	10대
Total	32대

표 3. 위협경보 감소 결과

기간	N-IDS 위협경보	제안 시스템	VAS 연관 위협경보	감소율
2004-01-20	1,037	30	1	97.1
2004-01-22	111	3	0	97.3
2004-01-23	122	4	0	96.7
2004-01-24	238	11	0	95.4

또한, 실험기간 중 측정한 서버관련 위협 중 대부분은 직접 상관되는 취약점이 없었고, 이는 알려진 취약점에 대한 사전 패치 작업이 충실히 이루어진 결과로 분석되었다. 전체 N-IDS 발생 로그 중 서버관련 위협과 네트워크관련 위협의 비율은 측정일에 따라 다소 차이는 있으나 [6 : 4] 정도로 측정되었다.

제안하는 시스템에서는 위협경보 발생과 관련하여 위협대상 자산의 관점에서 해당 자산에 대한 위협발생 형태와 위험발생 가능성을 확인할 수 있도록 (그림 9)과 같은 형태로 로그분석 결과를 표시한다.

(그림 9)에서 심각도가 최상(Critical)으로 나타난 자산에 가해지는 위협의 상세내역을 보기 위해 해당 자산정보를 확장하면 (그림 10)과 같이 시간순서에 따른 위협발생 상황을 상세하게 볼 수 있다.

(그림 10)에서 위협수준이 일정수준을 넘으면, 자산관리 DB와 연동하여 자산가치 정보(서비스 예상 손실액)를 제공해 준다. 운용자는 (그림 10)의 정보를 이용하여 일련의 위협이 어디에서 발생하는 지를 파악하고, 어떤 위험을 발생시킬 것인가에 대한 추론할 수 있다.

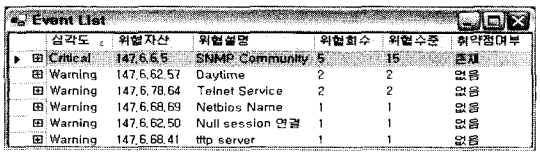


그림 9. 자산을 기준으로 한 위협정보 화면

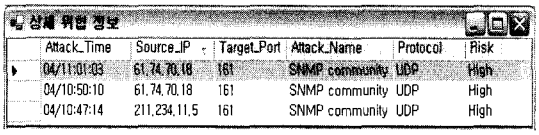


그림 10. 상세 위협 정보

Ⅵ. 결론 및 향후 연구방향

기존의 위험분석 방법론을 구현한 대부분의 시스템들은 개별 자산의 취약점 및 위협요인을 관리적, 물리적, 기술적 측면까지 광범위하게 고려하여 반영할 수 있도록 분석절차와 수단을 제공하고 있다. 그러나 자산의 소프트웨어적인 취약점과 사이버상의 위협요인 변동에 따른 자산의 위험수준을 실시간으로 산정하는 기능을 제공하지는 못하고 있다. 따라서, 네트워크 자산에 발생할 수 있는 위험에 신속히 대응해야 하는 ISP 보안관리자의 입장에서는 위험발생 요인의 변화를 지속적으로 측정, 관리하고, 위험발생에 따른 예상 손실수준을 실시간에 가깝게 정량적으로 평가할 수 있는 새로운 방법이 필요하다.

본 논문에서는 이러한 문제의 해결을 위해 상용 N-IDS 및 VAS가 제공하는 정보들을 이용하여, 네트워크와 서버에 대한 위협을 효과적으로 탐지하고, 실시간으로 위험분석이 가능한 시스템을 구현하고, 설계 방안과 실험결과를 제시하였다.

제안하는 시스템은 상용 N-IDS와 VAS의 탐지정보를 외부 DB에서 연동하는 형태로 구현됨으로써 특정 솔루션에 독립적으로 시스템을 구현하는 것이 가능하다. 또한 N-IDS와 VAS 탐지정보의 연관성을 이용하여 자산에 직접적인 위협정보만을 선별, 제공할 수 있어 불필요한 경보 정보로 인한 보안 운용자의 대응 부담을 크게 줄일 수 있고, N-IDS와 VAS의 탐지정보를 조합하여 다양한 보안관리 정보를 만들 수 있다는 것이 특징이다.

실험을 통해 기존의 N-IDS 탐지정보를 서버에 대한 위협과 네트워크에 대한 위협으로 분리하고, N-IDS와 VAS의 탐지정보를 상호 연동할 경우, 개별적으로 운용할 경우에 비해 경보 오류정보를 90% 이상 줄일 수 있음을 입증하였다. 또한, 위협탐지 능력과 위협속성에 대한 분석기능의 향상을 통해 실시간으로 위협발생에 따른 예상 위험수준을 산정할 수 있도록 시스템을 구성하였다.

향후, 표준 데이터 전달 포맷인 IDMEF(Intrusion Detection Message Exchange Format)에 대한 적용 연구, 위협경보의 최적화를 위해 개별 시스템 로그와의 연관성 분석 및 위협경보의 단계구분을 위한 기준치 설정방법 등에 대한 연구를 통해 위험분석의 정확도를 개선해 나갈 예정이다.

참 고 문 헌

[1] CSE, "A Guide to Security Risk Management for IT Systems", *Government of Canada, Communications*

Security Establishment, 1996.

[2] ISO/IEC TR 13335, Part 3, "Techniques for the management of IT Security", 1998.

[3] 한국전산원, "위험분석 방법론 및 자동화 도구(HAWK) 기술이전 교육 교재", 1998.9

[4] British Standards Institution(BSI), BS7799, 1999.

[5] ISO/IEC ,"Code of Practice for information Security Management", ISO/IEC 17799, 2000.

[6] TTA, "공공정보시스템 보안을 위한 위험분석 표준-위험분석 방법론 모델", TTAS. KO-12. 0007, 2000.3

[7] TruSecure Corporation, "A Practical Approach to a comprehensive Security Program", Hurwitz Report, 2001.

[8] CRAMM,"A Practioner's View of CRAMM", http://www.gammassl.co.uk/.

[9] OCTAVE, "OCATVE Criteria, Version 2.0", *Carnegie Mellon Software Engineering Institute, Dec.* 2001.

[10] KT, "정보보호 통합 컨설팅 지원시스템(KT-MECIA)", 2002.12

[11] Wenke Lee, Salvatore K.Stolfo," Data Mining Approaches for Intrusion Detection", Proceedings of the 7th USENIX Security Symposium, Jan. 1998.

[12] F.Cuppens,"Correlation in an intrusion detection process", Internet Security Communication Workshop (SECI02), Tunis-Tunisia, Sep. 2002.

[13] A.Valdes and K. Skinne,"Probabilistic Alert Correlation", 4th International Workshop on the Recent Advances in Intrusion Detection, Davis, USA, Oct. 2001.

[14] 이은영 외 5 명, "N-IDS에서 False Positives를 줄이기 위한 동적 중요도 계산 방법에 대한 연구," 정보보호학회지, 제 13권, 제 1호, pp. 22-31, 2003년 2월.

[15] 이수진 외 7명, "침입탐지 정보의 연관성 분석 시스템 설계 및 구현", *CISC-W'03 Proceedings*, pp. 28-38, 2003. 12

[16] Ron Gula, "Correlating IDS Alerts with Vulnerability Information", http://www.tenablesecurity.com.

[17] Internet Security Systems, "RealSecure SiteProtector 2.0", http://www.iss.net/.

[18] 문호건, 최진기, "네트워크의 자산, 취약점 및 위협의 상관성을 이용한 N-IDS Log 최적화 시스템 설계," *CISC-W'03 Proceedings*, pp. 153-159, 2003년 12월

[19] 이글루시큐리티, "SPiDER-TM", http://www.igloosec.co.kr/

[20] 한국정보보호진흥원, "취약점분석.평가를 위한 자산분석 지침(안)", 2001.9.

[21] 우병구 외 2명, "정보통신망의 효율적 보안관리를 위한 비즈니스 프로세스 기반의 자산평가 모델 및 방법론에 관한 연구", 한국정보처리학회, Vol 10-C권 4호, pp423-432, 2003.8

[22] 박현우 외 2명, "시스템 단위의 정량적 위험분석 도구 개발", 한국정보과학회 추계학술발표대회 논문집(I), 제 30권 제 2호, pp871-873, 2003.10

[23] 문호건, 이종필, "ISP의 네트워크 보안 위험을 고려한 예상 자산손실 모델링," CISC-W'03 Proceedings, pp. 121-127, 2003년 12월

[24] KT, "KORNET망 트래픽 측정 및 분석 보고서", 2003

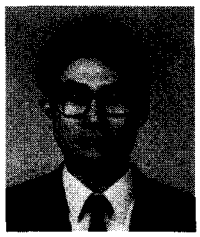
[25] KT, "KORNET망 설계기준", 2003.10.

[26] 문호건, "ISP 네트워크의 정량적 위험분석을 위한 자산가치 평가 방법 연구보고서", KT 기술연구소, 2004. 1

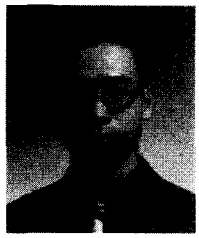
[27] ICAT, http://icat.nist.gov/icat.cfm

[28] Wins Technet, "스나이퍼 IDS 3.0 관리자 설명서", 2003

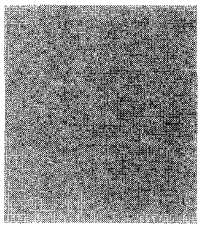
〈著者紹介〉



문 호 건 (Ho-Kun Moon) 정회원
1985년 2월: 숭실대학교 전자공학과 졸업
1987년 2월: 중앙대학교 전자공학과 석사
1987년 2월~현재: KT 기술연구소 네트워크보안연구실장
〈관심분야〉 네트워크 보안, 위험분석 등



최 진 기 (Jin-gi Choe) 비회원
1998년 2월: 숭실대학교 전자공학과 졸업
1999년 2월~현재: KT 기술연구소 네트워크보안연구실 전임연구원
〈관심분야〉 네트워크 보안



김 형 순 (Hyung-Soon Kim) 비회원
1983년 2월: 서울대학교 전자공학과 졸업
1984년 2월: 한국과학기술원 전기 및 전자공학과(박사과정 조기진학)
1989년 2월: 한국과학기술원 전기 및 전자공학과 박사
1987.1~1992.6: 디지콤정보통신 선임연구원
1992.7~현재: 부산대학교 전자공학과 부교수
〈관심분야〉 음성 신호처리, 정보보호