네트워크의 자산, 취약점 및 위협의 상관성을 이용한 N-IDS Log 최적화 시스템 설계

문호건*, 최진기*

*KT 기술연구소 차세대기술연구팀 인터넷보안연구실

Design of N-IDS Log optimization system using correlativity of asset, vulnerability and threat

Ho Kun Moon*, Jin Gi Choe*

*Internet Security Division, Next Generation Technology Team, KT Technology Laboratory

요 약

수 많은 정보자산들이 네트워크를 통해 연결된 환경에서 사이버 공격으로부터 정보자산들을 효과적으로 방어하기 위한 기본적인 수단으로 네트워크 침입탐지 시스템과 취약점 분석 시스템이 활용되고 있다. 그러나 네트워크 보안을 위해 개별적으로 운용되고 있는 네트워크 침입탐지 시스템과 취약점 분석 시스템이 보안관리 측면에서 오히려 보안 운용자의 부담을 가중시키는 요인으로 작용하고 있는 것이 현실이다. 따라서, 본 연구에서는 네트워크 보안 관리에 필수적인 정보 요소인 네트워크 자산, 취약점 및 위협이 갖는 의미와 상관성을 분석하고, 네트워크 침입탐지 시스템과 취약점 분석 시스템이 제공하는 정보들을 상호 연동하여 네트워크 침입탐지 시스템이 탐지하는 불필요한 경보정보의 양을 대폭 줄여 Log관리를 최적화할 수 있는 시스템을 구축하기 위한 설계 방법을 제시하였다.

I. 서론

최근 네트워크 상의 정보자산과 서비스가 정상적인 동작을 하는데 악영향을 미칠 수 있는 다양한 형태의 사이버 공격이 증가함에 따라 이로 인한 피해의 규모와 범위도 급속히 확대되고 있다. 이 같은 공격을 사전에 예방하고 공격을 효과적으로 탐지하여 네트워크를 통해 이루어지는 각종 서비스에 미치는 부정적인 영향(Impact)을 최소화하기 위한 연구가 활발히 진행되고 있다.

네트워크를 통해 연결된 수 많은 정보자산들을 사이버 공격으로부터 효과적으로 방어하기 위해서는 보호하고자 하는 정보자산에 대해 (1) 취약성과 이들 취약성을 위협하는 요인을 파악하고, (2) 이 같은 정보를 기반으로 정보자산의 보안현황을 파악하고, (3) 대응수준과 범위를 결정하는 실질적인 수단이 필요하다.

그러나, 대부분의 네트워크에서 보안을 위한 기본 장비로 도입, 운용되고 있는 네트워크 침입탐지 시스템(Network Intrusion Detection System, 이하 N-IDS)은 네트워크상의 불법적인 트래픽 감시를 위한 뛰어난 기능에도 불구하고 네트워크 자산 정보와 침입탐지 정책을 효과적으로 연동하지 못해 불필요한 많은 경보 정보들을 제공하여 보안관리자의 운용부담을 증대시키고 있다. 이로 인해, N-IDS는 당초의 불법적인 트래픽 감시 목적보다 보안사고 발생시 사고원인 파악 및 트래픽 분석 용도로 활용되고 있으며, 심지어 N-IDS의 무용론이 대두되고 있는 실정이다.[1]

이 같은 문제를 해결하기 위한 기존의 방법으로 N-IDS자체의 탐지 정확도를 향상시키는 방법[2][3][4][5]이 있으나 네트워크 자산의 취약점과 연관된 위협정보를 선택적으로 제공하지 못하고, 보안관제 전문업체를 중심으로 통합보안관리 시스

템(Enterprise Security Management system, 이하 ESM)을 써서 개별적인 보안장비들로부터 생성되는 정보들을 통합하여 분석하는 방법에 대한 연구를 하고 있으나[6] 장비투자와 운용에 따른 경제성의 문제 등으로 인해 네트워크 자산 및 취약점과 직접적인 관계가 없는 무의미한 경보 정보를 효과적으로 줄일 수 있는 수단으로 활용하는데 한계를 지니고 있다.

또한, 네트워크 자산의 취약점을 분석하기 위한 취약점 분석 시스템(Vulnerability Analysis System, 이하 VAS)의 경우, 대부분 보안 시스템 도입을 위한 컨설팅 또는 보안 감사(Audit) 과정에서 주로 사용되며[7], 네트워크상에서 운용되는 각종 시스템 또는 소프트웨어에 있을 수 있는 보안상의 취약점에 관한 정보를 찾아내고, 분석결과를 제공하는 역할을 한다.[8][10]

그러나, 네트워크 정보자산의 환경이 끊임없이 변화하는 상황에서는 특정 시점에서 분석한 취약점의 수준은 결코 현재의 취약점 수준을 정확히 반영하고 있다고 할 수 없다. 결국, 기존의 방식대로 네트워크 자산의 취약점과 위협정보를 별도로 관리할 경우, 보안관리 측면에서 불필요한 경보정보의 과도한 생성으로 인해 정작 필요한 정보를 얻는데 방해가 되므로 효과적인 보안관리가 어려워지게 된다.

따라서, 본 연구에서는 문제의 해결을 위해 네트워크의 자산과 자산이 갖는 취약점 및 취약점에 대한 위협의 상관성을 보안관리의 관점에서 정의하고, 현재 네트워크 상에서 개별적으로 운용되고 있는 네트워크 침입탐지 시스템과 취약점 분석 시스템의 상호 연동을 통하여 네트워크 침입탐지 시스템이 탐지하는 불필요한 경보정보의 양을 대폭 줄여 Log관리를 최적화할 수 있는 방법과 각 시스템 벤더와 독립적으로 네트워크상에서 경제적으로 구축, 운용할 수 있는 연동 시스템의 설계 방법을 제시한다.

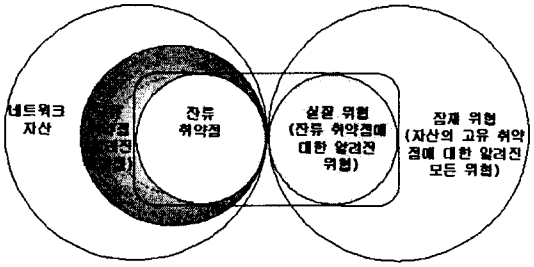
II. 본론

1. 자산, 취약점 및 위협의 관계

네트워크 보안정보의 분석에서 네트워크 자산은 네트워크를 구성하는 라우터, 스위치 등의 정보전달 장치와 서비스 처리 및 운용관리를 위한 각종 시스템을 말한다. 자산은 통상 네트워크 관리자가 자산관리 DB로 관리하며, 본 연구에서는 VAS와 자산 DB의 연동을 통해 네트워크에 접속되어 운영되고 있는 시스템의 정보를 이용한다.

네트워크상의 정보자산은 알려진 또는 알려지지 않은(Known/Unknown) 소프트웨어 취약점을 가지고 있으며, 이들 취약점은 대표적으로 미국 NIST(National Institute of Security Technology)에서 ICAT이란 Meta DB의 형태로 관리하며, 이들 DB는 다시 CVE(Common Vulnerability and Exposure) ID가 부여된 정제된 형태의 DB로 가공되며[11], N-IDS나 VAS업체는 이들 DB와 알려진 다양한 취약점 정보들을 이용하여 관련 시스템의 DB를 구축한다.

본 연구에서는 네트워크 위험분석을 위해



(그림 1) 자산, 취약점 및 위협의 관계

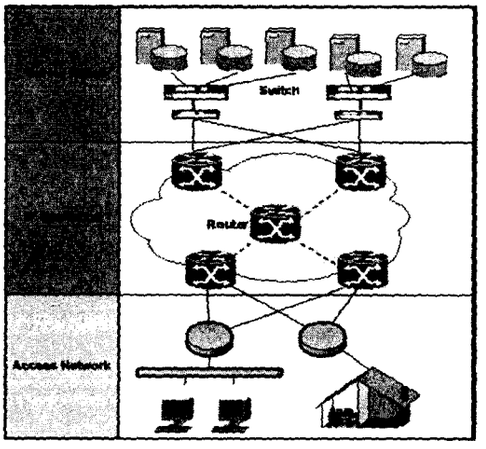
N-IDS 및 VAS 시스템의 DB를 이용하므로 알려진 취약점에 대해서만 다루며, 알려지지 않았던 취약점과 위협패턴이 새롭게 나타나면 N-IDS 및 VAS 시스템 벤더들은 각 시스템 DB의 갱신을 통해 취약점을 추가한다.

네트워크 보안관리 측면에서 자산, 취약점 및 위협의 상관성에 따라 (그림 1)과 같이 나타낼 수 있으며, 다음과 같이 구분, 정의할 수 있다.

1) 자산(Asset)

일반적으로 자산이라 함은 조직에 가치를 갖는 모든 것으로 정의하고, 그 분류 방법도 다양하게 제시되고 있으나[8][12][14], 본 연구에서는 네트워크가 제공하는 기본적인 서비스인 정보유통 기능을 제공하는 전송장비와 정보처리 기능을 제공하는 네트워크 상의 각종 시스템들로 한정한다. 이들 자산들로 구성되는 네트워크의 기본적인 모델은 (그림 2)와 같다.

본 네트워크 모델은 TCP/IP 기반의 3 계층 구조를 갖는 일반적인 네트워크 모델을 나타낸다.



(그림 2) TCP/IP 기반 네트워크 모델

본 연구에서는 각 계층별로 정보유통 및 정보전송 기능을 갖는 물리적인 시스템들을 자산범위에 포함하며, 무형적인 자산은 고려하지 않는다.

2) 취약점(Vulnerability)

네트워크 정보 자산의 취약점 역시 그 정의와 분류방법은 다양하지만[8][12], 본 연구에서는 시스템이 비정상적인 동작을 수행하도록 하는데 악용될 수 있는 소프트웨어적인 결함이라고 정의한다.[14] 네트워크상의 각종 정보자산이 가질 수 있는 소프트웨어적인 고유 취약점과 네트워크상에서 운용되고 있는 자산의 종류 및 각 자산의 잔류 취약점에 관한 정보는 VAS를 통해 알 수 있다. 본 연구에서는 시스템의 운용에 따른 취약점의 속성을 다음과 같이 분류하였다.

· 전체 취약점(V1) : 모든 정보시스템이 가지고 있는 알려진(Known) 전체 취약점으로 취약점 분석 시스템에 DB로 저장되어 있다.

· 고유 취약점(V2) : Network에서 운용되고 있는 정보 자산(Asset)의 알려진 모든 소프트웨어적인 취약점을 말하며, VAS의 DB로 관리된다.

$EV(Essential\ Vulnerabilities)=\{e_1, e_2, e_3, \cdots, e_n\}$

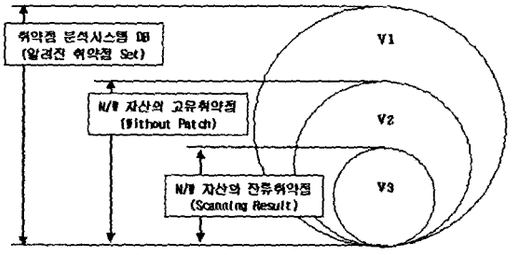
(여기서 e_i는 고유의 취약점)

· 잔류 취약점(V3) : Network에서 운용되고 있는 정보 자산(Asset)에 대해 VAS를 통해 찾아낸 취약점이며, 보안 패치 등을 통해 보안취약점이 개선되고 난 상태를 말한다. 대부분의 경우, 취약점이 알려지고 관련 패치가 되기 전까지 남아있는 취약점이며, 고유 취약점보다 같거나 작은 집합으로 나타난다.

$RV(Remained\ Vulnerabilities)=\{v_1, v_2, v_3, \cdots, v_k\}$

(여기서 v_i는 잔류취약점, $v_k : e_n \quad k < n$)

$EV \supseteq RV$ (등호의 경우는 시스템이 패치가 되지 않고 원형 그대로 존재하는 경우)



(그림 3) 취약점의 구분

VAS가 관리하는 취약점 DB 중 네트워크 자산과 개별 자산에 잔류한 취약점의 관계는 (그림 3)과 같이 나타낼 수 있다.

3) 위협(Threat)

위협은 정보자산에 바람직하지 않은 영향을 줄 수 있는 잠재적인 요인으로 정의할 수 있으며, 이 같은 위협이 현실적으로 발생하면 공격으로 인식한다.[15] 따라서, N-IDS에서 관리하는 위협 DB는 잠재적인 위협으로 볼 수 있으며, N-IDS에서 탐지한 위협은 네트워크에 대한 공격이 발생한 것으로 볼 수 있다. 위협은 네트워크에 미치는 영향에 따라 다음과 같은 속성을 갖는 요소들로 분류할 수 있다. 이 같은 상관관계는 (그림 4)와 같이 나타낼 수 있다.

· 전체 위협(T1) : 알려진(Known) 전체 위협으로 침입탐지시스템(IDS)에 DB로 관리된다.

· 잠재 위협(T2) : 특정한 네트워크 자산의 알려진 모든 취약점 즉 고유 취약점을 이용하여 공격(Attack)할 수 있는 알려진 모든 공격코드(Exploit Code)를 말한다.

$PT(Potential\ Threats) = \{t_1, t_2, t_3, \cdots, t_m\}$

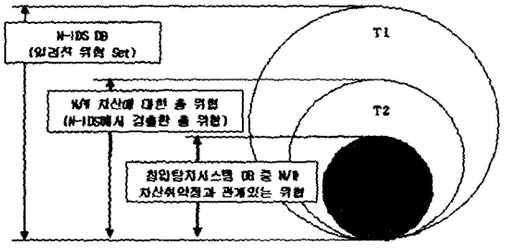
(여기서 t_i는 잠재위협, $v_k : e_n : t_m \; k < n < m$)

· 실질 위협(T3) : 네트워크 침입탐지 시스템에서 탐지한 공격코드(Alarm Signal) 중 네트워크상에 존재하는 자산의 잔류 취약점과 직접적인 상관성이 있는 공격코드이며, 보안 담당자의 즉각적인 대응이 필요한 위협이다.

$RT(Real\ Threats) = \{t_1, t_2, t_3, \cdots, t_m \mid RV\}$

$PT(m) \rangle\ RT(m)$ ($PT(m)$은 잠재위협의 개수, $RT(m)$은 실질위협의 개수)

잔류 취약점(V3)과 실질 위협은 네트워크 자산에 직접적인 손실요인(Risk)을 발생시킬 수 있는 원인으로 작용한다. 이들 각각의 정보를 개별적으로 산출하는 N-IDS와 VAS 시스템을 실시간 연동하면, 네트워크 취약수준의 변화를 관찰할 수 있고 IDS의 불필요한 보안 경보신호(False Positive)를 대폭 줄일 수 있게 된다. 또한, 자산의



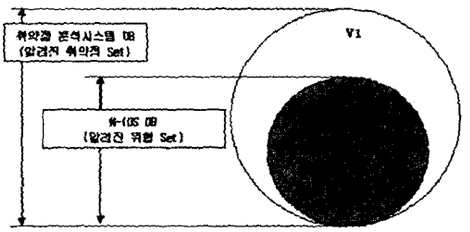
(그림 4) 위협의 구분

가치정보와 연동하면 네트워크의 위험수준(Risk level)을 정성적, 정량적으로 해석하고, 관리할 수 있게 된다.

4) 취약점과 위협의 관계

일반적으로 특정한 취약점에 대해 다수의 위협이 상관되며, 취약점과 위협의 상관관계는 (그림 5) 및 (그림 6)과 같이 나타낼 수 있다. 통상 취약점이 발견되고(Discovered), 발표되어도(Announced) 해당 취약점을 공격하는 위협은 일정한 시간 후 출현하므로(Happen) 취약점 분석 시스템의 취약점 DB 중 IDS의 DB와 직접적인 관계가 없는 것들이 다수 있을 수 있다. 따라서, 현재 직접적인 위협이 알려지지 않은 취약점, 즉 취약점을 공격할 수 있는 공격코드(Exploit code)가 알려지지 않은 취약점은 유형(Availability, Integrity, Confidentiality)에 따라 해당 분야의 잠재 위험 요소로 인식할 수 있다.[8]

정보자산에 내재한 취약점의 존재는 잠재적인 위협을 현실화시킬 수 있는 역할을 하며, 취약점을 제거하면 취약점을 이용한 대부분의 위협은 네트워크 자산에 실질적인 손실을 줄 수 없다. 이 같은 자산, 취약점 및 위협의 상관성을 이용하여 네트워크 침입탐지 시스템에서 탐지한 전체 경보 신호 중 네트워크 자산 및 자산의 취약점과 직접적

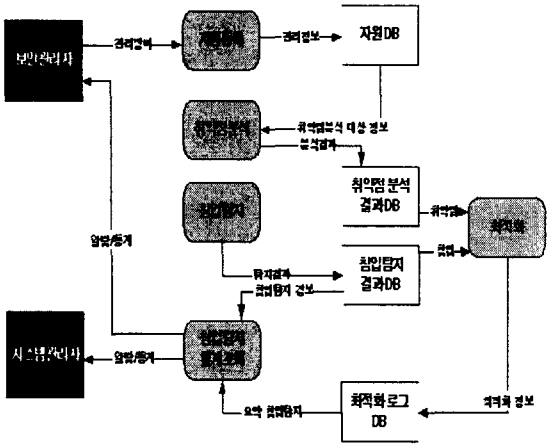


(그림 5) 취약점과 위협의 관계

인 상관성에 따라 분류함으로써 불필요한 경보를 대폭 줄이고, 네트워크 보안 관리자가 직접적으로 대응할 필요가 있는 경보만 제공할 수 있다.

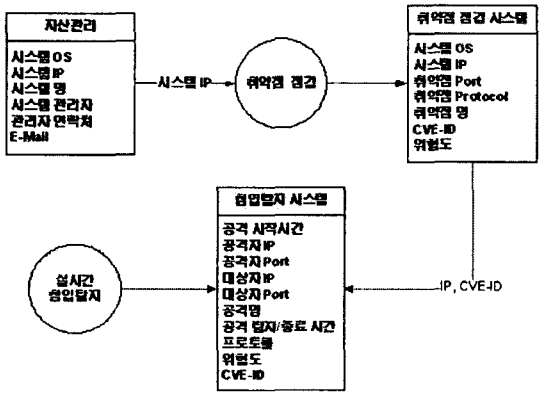
2. 시스템 구현 방향

본 연구에서는 특정 솔루션 벤더의 N-IDS와 VAS 시스템에 독립적으로 구현 가능한 형태로 시스템을 설계하였으며, 각 시스템의 정보연동을 외부 DB에서 수행하므로 N-IDS 시스템 자체의 자산관련 정책을 별도로 설정, 갱신할 필요가 없이 네트워크로 유입되는 전체 트래픽으로부터 일상적인 유해 패킷의 총량과 네트워크 자산에 직접적으로 영향을 미칠 수 있는 유해 패킷에 관한 정보를 동시에 관리할 수 있도록 하였다. (그림 6)은 시스템 로그 및 경보 정보 발생 개념도를 나타내며, (그림 7)은 자산, 취약점 및 위협정보를 관리하는 각 시스템간의 데이터 상관관계를 나타낸다.



(그림 6) 시스템 로그 및 경보 정보 발생 개념도

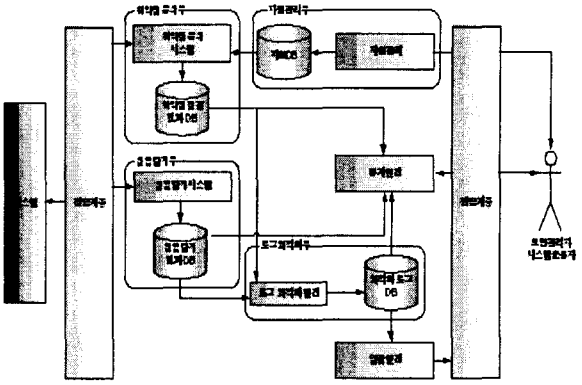
VAS는 자산정보를 이용하여 자산이 현재 가지고 있는 취약점을 점검하고 이러한 취약점 점검 결과는 N-IDS의 경보정보를 정제하는데 사용할 수 있다. 즉 현재 자산이 가지고 있는 취약점과 관련이 있는 경보정보에 대해서만 선택적으로 감시할 수 있도록 한다. 이때 VAS와 N-IDS간의 정보를 서로 연관시키는 키 정보로서는 CVE-ID나



(그림 7) 자산, 침입탐지 및 취약점 정보간 데이터 상관관계

IP가 될 수 있다.

네트워크 상에서는 자산, 취약점 및 위협정보를 관리하는 각각의 시스템들이 (그림 8)과 같이 연동된 형태로 동작하며, 각각의 정보를 관리하는 기능들을 모듈화하여 구성하여 개별 시스템이 특정한 밴더의 제품과 무관하게 구현될 수 있도록



(그림 8) 네트워크 침입탐지 경보 취적화 시스템 구성도

하였다.

네트워크 상에서는 자산, 취약점 및 위협정보를 관리하는 각각의 시스템들이 (그림 8)과 같이 연동된 형태로 동작하며, 각각의 정보를 관리하는 기능들을 모듈화하여 구성하여 개별 시스템이 특정한 밴더의 제품과 무관하게 구현될 수 있도록 하였다.

네트워크 침입탐지 경보 최적화 시스템의 동작은 다음과 같다.

(1) 시스템운용자가 자원관리부의 자원등록 인터페이스를 이용하여 보안관리 대상 시스템을 입력한다. 이 데이터는 자원DB에 저장이 되며 취약점 분석부로 보내어져 취약점 분석이 수행된다.

(2) 침입 탐지부는 시스템의 침입정보를 탐지하여 침입탐지 DB에 저장하게 된다.

(3) 로그 최적화부는 취약점 분석결과 DB와 침입탐지결과 DB를 이용하여 현재 네트워크의 자산과 관련이 없는 알람정보를 필터링하게 되는데 현재 시스템이 가지고 있는 취약점 분석 결과를 참고하여 이와 관련이 없는 침입탐지 알람에 대해서는 통계생성시 참고 할 수 있도록 통계엔진에 보내어지고 걸러진 정보만 알람을 발생시킬 수 있도록 알람 엔진으로 보내진다.

(4) 이렇게 하여 시스템 운용자 및 보안관리자가 잘못 발생된 알람에 대하여 대응하는 부담을 줄일 수 있도록 하며 침해사고에 좀더 효율적으로 대응할 수 있도록 한다

(5) 발생되는 알람은 자원등록과정에서 입력된 자산정보를 고려하여 보안관리자 혹은 시스템 관리자가 침입대응 우선 순위를 판단할 수 있도록 한다.

이상 설명한 바와 같이 취약점 분석 시스템의 분석 결과와 침입탐지 시스템을 서로 연동하여 불필요한 알람 및 로그를 걸러줌으로써 로그 분석 및 관리의 효율과 네트워크 침입탐지 시스템의 오탐률을 개선하여 시스템 운용자 및 보안관리자가 침해사고에 좀 더 효율적으로 대응할 수 있도록 하는데 효과가 있다.

III. 결론

수 많은 정보자산들이 네트워크를 통해 연결된 환경에서 사이버 공격으로부터 정보자산들을 효과적으로 방어하기 위한 기본적인 수단으로 N-IDS와 VAS 가 활용되고 있다. 그러나 네트워크 보안을 위해 개별적으로 운용되고 있는 N-IDS 와 VAS 가 보안관리 측면에서 오히려 보안 운용자의 부담을 가중시키는 요인으로 작용하고 있어 시스템의 효과적인 활용방법을 찾는 것이 시급한 과제가 되고 있다.

따라서, 본 연구에서는 네트워크 상의 자산과 그 자산이 갖는 소프트웨어적인 취약점 및 취약점을 이용하는 각종 위협의 상관성을 보안관리의 관점에서 재정의하였으며, 네트워크 보안을 위해 그동안 개별적으로 운용되던 VAS와 N-IDS 가 현장에서 보안관리자의 운용부담만 증가시키고 실질적인 보안 대응효과를 제공하지 못하는 문제를 개선하기 위한 시스템적 접근 방법을 제시하였다.
시스템의 구현을 위해 기존의 상용 VAS와 N-IDS를 이용하였으며, VAS와 N-IDS 시스템의 정보를 외부의 DB를 이용하여 상호 연동함으로써 시스템 밴더와 독립적으로 관련 시스템체계를 구현하는 것이 가능하고, N-IDS와 VAS를 이용한 다양한 보안정보 분석작업을 할 수 있게 되어 각 시스템의 기능을 다양하게 활용할 수 있게 하였다.

시스템의 동작원리는 자산관리 정보를 기초로 VAS 시스템에서 찾아낸 네트워크 정보자산의 취약점 정보를 N-IDS 시스템에 제공하고, N-IDS 시스템은 네트워크 상의 각종 사이버 공격 탐지 정보 중 VAS 시스템이 제공한 정보자산의 취약점과 직접적인 상관성을 갖는 사이버 위협 또는 공격 탐지 정보만을 선별, 제공함으로써 잘못된 경보 정보로 인한 보안 운용자의 대응 부담을 크게 줄일 수 있고, VAS 와 N-IDS 가 제공하는 정보를 조합하여 다양한 보안관리 정보를 만들 수 있다는 것이 특징이다.

본 시스템은 N-IDS가 운용되는 IDC(Internet Data Center), 서버팜(Sever Farm) 등에 적용할 경우, 유용성이 매우 클 것으로 판단되며 직접적인 실험을 통해 시스템 구조와 관리 정보의 설계를 개선해 나갈 필요가 있다.
향후, 본 시스템을 자산의 가치 평가모델과 함께 취약점과 위협의 수준을 수치적으로 산정할 수 있는 방법과 연동할 경우, 네트워크의 위험수준(Risk level)을 정성적, 정량적으로 해석하고, 관리할 수 있는 시스템으로 발전시켜 나갈 수 있게 된다.

참고문헌

[1] Gartner, "IDS a Failure, Firewalls Recommended," WEB HOST INDUSTRY REVIEW, June 11.
[2] Chris Sinclair, Lyn Pierce and Sara Matzner, "An Application of Machine Learning to Network Intrusion Detection".
[3] Jun-Zhong Zhao and Hou-Kuan Huang, "An Intrusion Detection System based on Data Mining and Immune Principles", IEEE Proceedings on Machine Learning and Cybernetics., pp. 524-528, Nov. 2002.
[4] Yan Qiao and Xie Weixin , "A Network IDS with Low False Positive Rate", IEEE pp. 1121-1126, 2002.
[5] Constantine Manikopoulos and Symeon Papavassiliou, "Network Intrusion and Fault Detection: A Statistical Anomaly Approach", IEEE Comm. Magazine pp 76-82, 2002.
[6] 이글루시큐리티, "ESM 동향 및 추세", 한국정보보호진흥원, 기획특집.
[7] 인젠, "보안컨설팅 방법론".
[8] 한국전산원(1998). 위험분석 방법론 및 자동화 도구 기술 이전 교육 교재.
[9] 고려대학교. "컴퓨터 해킹, 바이러스 피해액 산

출방법 연구", 한국정보보호진흥원 최종연구보고서, 2002.11.30.
[10] 한국정보보호진흥원(외). "취약성 점검기술 및 침입시도탐지기술 개발에 관한 연구", 정보통신부 연구개발 결과 보고서, 2002.12.
[11] http://icat.nist.gov/icat.cfm
[12] 최상수, 방영환, 최성자, 이강수, "보안관리 및 위험분석을 위한 분류체계, 평가기준 및 평가 스케일의 조사연구", 한국정보보호학회지, 13권 제 3호, pp. 38-49, 2003년 6월.
[13] Gary Stoneburner, Alice Gogune, and Alexis Feringa, "Risk Management Guide for Information Technology Systems", NIST(National Institute of Standard and Technology), Special Publication 800-30.
[14] 한국정보보호진흥원, "취약점 분석.평가를 위한 자산분석 지침(안)", 2001.9.
[15]Edward G. Amoroso, "Fundamentals of Computer Security Technology", AT&T Bell Lab.