情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

취약점과 위협의 상관성 분석을 통한 네트워크 위험 조기경보 시스템 설계

문 호 건*, 최 진 기*, 강 유*, 이 명 수*

요 약

기업 활동에서 인터넷과 정보통신 시스템에 대한 의존도가 점차 심화됨에 따라 보안사고의 발생시 기업이 감당해야 할 사업적 위험도 함께 증대하고 있다. 따라서 최근 다양한 사이버 공격의 징후를 조기에 감지하고 대응함으로써 피해범위를 최소화할 수 있는 조기경보 체계의 구축에 많은 기업들이 관심을 갖기 시작했다. 하지만 조기경보 체계의 구축과 운용을 위해서는 비용과 기술적인 장애를 극복해야 한다. 본 논문은 대부분의 기업들이 네트워크에서 실시간 위협탐지를 위해 사용하는 네트워크 침입탐지 시스템(N-IDS)과 정기적인 보안감사용으로 주로 운영하는 취약점분석 시스템(VAS)을 이용하여 경제적이고, 효과적으로 사이버 공격의 징후를 신속하게 파악할 수 있는 조기경보 시스템의 설계방법을 제시하였다.

Ⅰ. 서 론

초고속 인터넷의 보급 확산과 IT 기술의 급격한 발전으로 우리 사회전반에서 인터넷에 대한 의존도는 지속적으로 증가하고 있다. 반면 인터넷을 이용한 사이버 커뮤니티, 전자우편 및 전자상거래 등이 보편화되면서 사이버상의 불법적인 행위로 인한 피해공간이 확대되는 부정적인 결과도 나타나고 있다.

최근 사이버 공격은 다음과 같은 특징을 갖는다. 첫째, 정치, 경제, 사회, 군사 및 산업적 목적 달성을 위한 수단으로 이용되는 사례가 늘어나고 있다. 둘째, 공격의 파급효과가 단시간에 광범위한 인터넷의 마비사태를 불러올 수 있는 형태로 진화하고 있다. 셋째, 보안 취약점(Vulnerability)의 공개와 이들 취약점을 악용한 악성코드(Exploit code)의 등장 간격이 점차 짧아지고 있다[13].

이와 같은 환경에서 사이버 공격의 징후를 나타내는 다양한 정보들을 효과적으로 파악하고, 피해로 직결될 수 있는 경보정보의 속성을 분석하여 조직내 보안 관리자에게 조기 경보함으로써 피해발생의 가능성과 범위를 최소화하는 일련의 능동적인 대응절차를 구축, 운영하는 것이 매우 중요하다.

기존의 조기 경보체제는 대부분 바이러스 백신업체로부터 바이러스 예·경보 서비스를 받거나 국내외 CERT(Computer Emergency Response Team) 또는 ISAC(Information Sharing & Analysis Center)와의 침해사고 대응 협력 등의 방법에 의존하고 있다. 지난 2003년 1월 25일 인터넷 대란 이후 대부분의 기업들이 네트워크를 통해 유통되는 비정상 트래픽을 감시, 차단하기 위해 다양한 보안장비들을 도입, 운용하는데 많은 비용을 쓰고 있다. 하지만, 네트워크에서 임의 시점에 사이버 공격의 징후를 신속하게 파악하는 것은 여전히 현실적인 어려움이 있다. 주된 이유는 각종 보안장비들이 제공하는 대량의 탐지정보(Log)들 간에 존재하는 상관성(Correlation)들을 분석하고, 가공하는 작업을 전적으로 보안 관리자의 수작업에 의존하고 있기 때문이다[4]. 최근 이와 같은 문제를 효과적으로 해결하기 위한 수단으로 ESM (Enterprise Security Management system)을 사용하는 경우가 점차 늘어나고 있다. ESM이 갖는 장점에도 불구하고 연동대상 시스템마다 서로 상이한 형태의 이벤트 정보 포맷을 통일된 형태로 변환하여 DB화 하는 과정이 복잡하고, 에이전트 설치에 따른 시스템의 기능 지원에 제약이 있으며, 네트워크 구성 환경

* KT 정보보호단 ({hkmoon, jingiya, yulguang, msrhee}@kt.co.kr)

에 따라 시스템 로그들 간의 상관성을 규정하는데 많은 시간이 소요되는 문제 등은 ESM 도입의 장애요인이 되고 있다. 따라서 네트워크의 자산구성이 자주 변동하고, 많은 이종 시스템을 보유하고 있으며, 자산변동 상태를 반영한 보안정책을 수립할 전문 보안인력이 부족한 경우에는 현실적으로 ESM을 운용하기가 어렵다.

사이버 공격의 징후를 조기에 탐지하기 위한 기존의 연구는 트래픽 추이 분석, 로그간 상관관계 분석, 허니넷 등이 있다. 각각의 연구가 지닌 장점에도 불구하고 구현에 따른 경제성과 공격의 유형을 다양한 형태의 정보로 가공, 분석할 수 있는 확장성 측면에서 상대적인 단점을 지니고 있다.

본 논문에서는 네트워크에서 실시간 위협탐지를 위해 사용되는 N-IDS(Network Intrusion Detection System)와 정기적인 보안감사(Security Audit)용으로 주로 운영되는 VAS(Vulnerability Analysis System)를 이용하여 효과적인 조기경보 시스템을 설계, 구현할 수 있는 방법을 제시한다. 시스템은 위협탐지 정보와 취약점 탐지정보를 별도의 DB를 통해 분석함으로써 위협과 취약점을 탐지하는 각 기능이 특정 벤더의 제품에 독립적으로 구현 가능할 수 있도록 설계하였다.

이하 본 논문의 구성은 다음과 같다. 2장에서는 기존의 조기경보 관련 연구들을 소개하고, 3장에서는 본 논문에서 제시하는 취약점과 위협정보의 속성분류 방법을 바탕으로 상관 속성을 설명한다. 4장에서는 N-IDS와 VAS의 탐지정보를 이용한 조기 경보시스템의 설계개념을 설명하고, 마지막으로 5장에서 결론과 향후 연구방향을 제시한다.

II. 관련 연구

1. 트래픽 추이 분석

이 기법은 네트워크 장비로부터 일정시간 간격동안의 트래픽 정보를 수집, 분석하여 정상 트래픽 패턴과 비교를 함으로써 현재 트래픽의 이상을 조기 경보한다. 이러한 트래픽 추이분석 방식은 트래픽 양(Volume)과 플로우(Flow) 분석[5-6]으로 나누어진다. 트래픽 양 분석은 라우터와 같은 네트워크 장비로부터 SNMP(Simple Network Management Protocol)를 이용하여 IP계층의 트래픽 양과 관련된 정보를 수집한다. 수집된 트래픽 양을 시간 또는 일자별로 설정된 변동 임계치(Variation threshold value)와 비교하여 이상 트래픽을 탐지해낸다. 이러한 방식의 경우 서비스 거부 공격(Denial of service)이나 웜(Worm) 같은 대량의 이상 트래픽 발생을 빠르게 탐지할 수 있으나 서비스 프로토콜별로 상세한 공격정보를 알 수 없기 때문에 별도의 트래픽 분석을 위한 장비가 추가적으로 필요하다는 단점이 있다.

플로우 분석은 송신자에서 수신자로의 일련의 단방향성 패킷의 흐름을 분석하는 것이다. 플로우는 서비스 접속 주소(송신자 주소, 송신자 포트 번호, 수신자 주소, 수신자 포트 번호), 호스트 주소(송신자 네트워크 주소, 수신자 네트워크 주소) 및 AS번호(송신자 AS 번호, 수신자 AS 번호)등의 정보를 포함하고 있다. 이러한 정보를 기반으로 서비스(포트 번호), 프로토콜(TCP, UDP, ICMP 등), 패킷 사이즈 분포, 출발지 및 목적지 주소[7-8] 등의 통계지표를 생성한 후 정상적인 트래픽 패턴과 비교하여 이상 트래픽을 탐지한다. 플로우 분석 방식은 트래픽 양 분석 방식에 비해 이상 트래픽을 보다 상세하게 분석, 탐지할 수 있는 장점이 있으나, 방대한 규모의 데이터 축적과 분석시스템의 구축에 많은 비용이 들며, 플로우 정보 수집으로 인해 해당 네트워크 장비의 성능을 저하시킬 수 있는 단점이 있다.

이상 언급한 네트워크 트래픽 추이분석 방식은 웜의 발생으로 인해 대량의 이상 트래픽이 발생하는 것을 탐지하기 용이하다는 장점이 있다. 그러나 정상적인 트래픽의 일시적인 폭주(Congestion) 현상과 웜 발생으로 인한 트래픽의 이상변화를 구별하기가 어렵고, 특정한 공격의 발생이 자산의 위험과 직결될 것인지에 대한 판단을 할 수 없다는 문제점이 있다. 즉 탐지 오류(False positive)가 발생하기 쉬워 보안 관리자의 부담이 커지고, 자세한 트래픽 분석을 위한 별도의 시스템 운용이 필요하다는 문제가 있다.

2. 로그간 상관관계 분석

네트워크상에서 운용되는 다양한 보안 장비(N-IDS, IPS, 방화벽 및 VPN 등)는 개별적인 형태의 침입탐지/차단 로그를 생성한다. 이러한 로그 데이터들 간의 상관관계를 분석하여 공격을 신속하게 탐지하는 방법에 대한 연구가 활발하다.

로그간 상관관계 분석 기법은 분산되어 있는 여러 장비들로부터 로그정보를 수집하여 이들 간의 상관성을 분석함으로써 위험발생 가능성을 보다 정확히 탐지하고, 위협요소를 예측하며 임박한 위협 경보를 신속히 전달하는 것을 목표로 하고 있다. 이 같은 기능을 지원하기 위해서는 네트워크상의 주요 관리대상 시스

템들에 위협을 탐지할 수 있는 센서기능을 갖는 에이전트(agent)를 두어야 하고, 서로 상이한 형태의 로그 포맷을 통일된 형태로 변환하여 관리해야 한다.

이 같은 개념을 구현한 대표적인 제품[9]으로 ESM이 있으나 정책설정 과정이 복잡하고, 서로 상이한 형태의 로그를 통일된 형태로 변환하는 정규화(Normalization)에 많은 시간이 소요된다. 또한 ESM이 다양한 로그를 기반으로 판단한 위협의 신뢰성 검증이 불가능하며, 위협발생 시 대책과 조치가 전적으로 보안 관리자의 판단에 의존해야하는 단점이 있다.

3. 허니넷(Honeynet)

로그간 상관관계 분석 기법은 위협탐지를 위한 특정한 규칙(rule)을 사용하기 때문에 패턴이 알려진 공격은 정상적으로 탐지할 수 있지만 알려지지 않은 새로운 공격은 탐지할 수 없다. 외부에 공개되지 않았지만 해커가 은밀히 사용하는 공격을 탐지하기 위한 방법 중 하나가 허니넷 분석이다.

허니넷은 '외부에서 용이하게 탐지, 공격 및 침해할 수 있도록 만들어진 보안 자원'으로 정의되는 허니팟(honeypot)[10]의 일종이다. 허니팟은 사이버 상의 비정상적인 공격행위가 용이하게 이루어질 수 있도록 고안되었기 때문에 허니팟으로 들어오는 모든 패킷이나 그 안에서 이뤄지는 행위는 사이버 공격 의도를 가진 자의 정탐(scanning)이나 침입 행위일 가능성이 높다. 허니넷은 출입하는 모든 트래픽을 모니터링하고 수집하며, 분석할 수 있는 엄격히 통제된 네트워크다. 이러한 통제된 네트워크로 출입하는 대부분의 트래픽은 악의적 의도를 갖는 트래픽이라 추정할 수 있다. 허니넷은 데이터를 통제, 수집, 및 분석하는 솔루션으로 구성된다. 데이터 통제는 snort inline과 rc. firewall 등이 사용되며, 데이터 수집은 snort, sebek, termlog 등이 사용된다. 데이터 분석을 위한 툴로서는 honeyinspector, privmsg 등이 많이 활용되고 있다.[11] 상용 허니넷으로 symantec의 decoy server[12]가 있으며 이는 공격자를 유도하고 모니터링하기 위한 다양한 방법을 제공한다.

허니넷은 외부에 알려지지 않은 새로운 공격을 탐지한다는 장점이 있지만 공격자의 어떤 행위가 실제 공격인지 여부를 보안 관리자의 주관적인 판단에 의존한다. 또한 보안 관리자가 수많은 탐지된 로그를 분석하는 것이 현실적으로 어렵고 관리자의 능력에 따라 공격 탐지 수준이 크게 달라진다는 문제점이 있다. 허니넷을 통해 수집되는 정보는 잠재적인 위협에 대한 경보정보를 제공하며, 운용중인 네트워크에 대한 직접적인 경보정보를 제공하는 것은 아니다.

Ⅲ. 네트워크 위험 구성 요소

네트워크에 발생되는 위험(Risk)을 신속하게 탐지하기 위해서는 위험을 구성하는 자산, 취약점 및 위협의 속성을 운용관점에서 각각 분석하고 이들 간의 상관관계를 재정의할 필요가 있다.

1. 자산

일반적으로 자산(Asset)이라 함은 조직에 가치를 갖는 모든 것으로 정의하고, 그 분류 방법도 다양하게 제시되고 있으나[13-15] 본 논문에서는 자산을 네트워크가 제공하는 기본적인 서비스인 정보유통 기능을 제공하는 전송장비와 정보처리 기능을 제공하는 네트워크 상의 각종 시스템들로 한정한다.

2. 취약점

자산의 취약점 역시 그 정의와 분류방법은 다양하지만[13-14] 본 논문에서는 시스템이 비정상적인 동작을 수행하도록 하는데 악용될 수 있는 소프트웨어적인 결함이라고 정의한다. 네트워크상의 각종 자산이 가질 수 있는 소프트웨어적인 취약점과 네트워크상에서 운용되고 있는 자산의 종류 및 각 자산의 잔류 취약점에 관한 정보는 VAS를 통해 알 수 있다. 본 논문에서는 자산의 운용에 따른 취약점의 속성을 다음과 같이 분류하였다.

- 전체 취약점(V1): 모든 자산이 가지고 있는 알려진 (Known) 전체 취약점으로 VAS의 DB로 저장되어 있다.
- 잠재 취약점(V2): 대상 네트워크에서 운용되고 있는 자산(Asset)의 알려진 모든 소프트웨어적인 취약점을 말한다.
- 잔류 취약점(V3): 잠재 취약점(V2) 중 보안 패치 등을 통해 제거되지 않고 남아있는 취약점이며, 잠재 취약점보다 같거나 작은 집합으로 나타난다.

이들 취약점간의 관계를 [그림 1]과 같이 나타낼 수 있다.

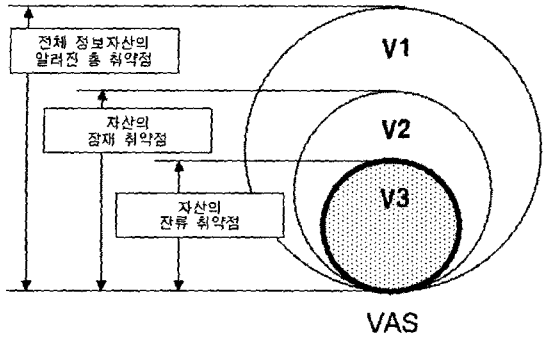


그림 1. 취약점의 구분

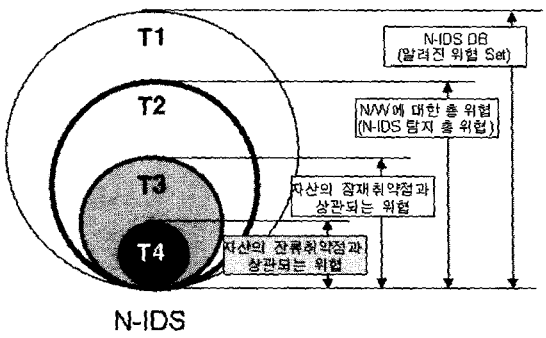


그림 2. 위협의 상관관계

3. 위협

위협은 자산에 바람직하지 않은 영향을 줄 수 있는 잠재적인 요인으로 정의할 수 있으며, 이 같은 위협이 현실적으로 발생하면 공격으로 인식한다.[16] 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 2]와 같이 나타낼 수 있다.[17-18]

- 전체 위협(T1): 알려진 전체 위협으로 N-IDS의 DB로 관리된다.
- 탐지 위협(T2): 대상 네트워크의 N-IDS에서 탐지한 모든 공격 코드를 의미한다.
- 잠재 취약점 상관 위협(T3): N-IDS에서 탐지한 공격코드 중 네트워크에 존재하는 자산의 잠재 취약점과 상관성이 있는 공격코드이며, 이러한 위협이 대량 발생할 경우 자산의 가용성 저하를 일으킬 수 있다.
- 잔류 취약점 상관 위협(T4): N-IDS에서 탐지한 공격코드 중 자산의 잔류 취약점과 직접적인 상관성 있는 공격코드이며, 보안담당자의 즉각적인 대응이 필요한 위협이다.

잔류 취약점(V3)과 잔류 취약점 상관 위협(T4)은 자산에 직접적인 위험을 발생시킬 수 있는 원인으로 작용한다. 이들 각각의 정보를 개별적으로 산출하는 N-IDS와 VAS 시스템을 실시간 연동하면, 네트워크 취약수준의 변화를 관찰할 수 있고 N-IDS의 불필요한 경보를 대폭 줄여 탐지 정확도를 향상시킬 수 있다.

4. 자산, 취약점, 위협의 상관관계

일반적으로 특정한 취약점에 대해 다수의 위협이 상관되며, 취약점과 위협의 상관관계는 [그림 3]과 같이 나타낼 수 있다. R1은 자산의 잔류 취약점(V3)에 대한 공격으로 실질적인 위험을 발생 시킨다. R2는 자산의 잠재 취약점(V2)에 대한 공격으로 자산에 잠재적인 위험이 된다. R3은 자산에 대한 간접 공격으로서 자산의 가용성을 저하시키는 위험으로 작용한다.

자산에 내재한 취약점의 존재는 잠재적인 위협을 현실화시킬 수 있는 역할을 하며, 취약점을 제거하면 취약점을 이용한 대부분의 위협은 자산에 실질적인 손실을 줄 수 없다. 이 같은 자산, 취약점 및 위협의 상관성을 이용하여 N-IDS에서 탐지한 전체 경보 중 자산 및 자산의 취약점과 직접적인 상관성에 따라 분류함으로써 불필요한 경보를 대폭 줄이고, 네트워크 보안 관리자가 직접적으로 대응할 필요가 있는 경보만 제공할 수 있다.

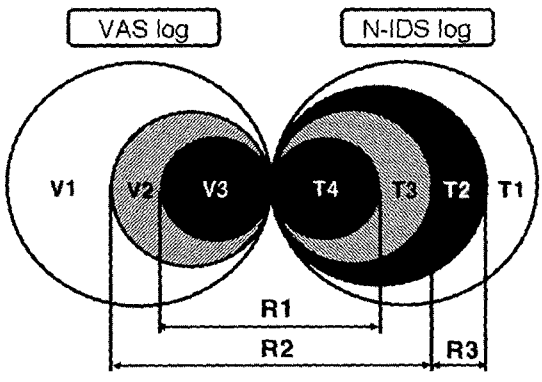


그림 3. 취약점과 위협의 관계

Ⅳ. 조기 경보 시스템 설계

1. 설계 고려 사항

본 논문에서는 자산, 취약점 및 위협의 상관관계 분석을 통해 자산에 발생할 수 있는 위험을 3가지로 분류했다.

- R1(실현 위험): 잔류 취약점에 대한 공격
- R2(잠재 위험): 잠재 취약점에 대한 공격
- R3(가용성 잠재 위험): 취약점과의 상관성이 없는 자산에 대한 가용성 저하 공격

제안한 시스템은 각각의 위험유형들을 빠르게 탐지할 수 있도록 위험의 특성별로 분석/탐지 모듈을 설계하였다. 또한, 상용 N-IDS와 VAS를 각각 네트워크 상의 위협정보와 자산의 취약점 정보를 수집하는 수단으로 활용하며, SNMP 프로토콜을 이용하여 각 시스템의 로그를 수집하는 수단으로 활용하였다. 각 시스템간의 정보연동은 외부 DB에서 수행함으로서 특정 솔루션 벤더의 시스템에 독립적으로 구현 가능하도록 설계하였다.

2. 시스템 구조

본 논문에서 제안하는 시스템은 [그림 4]와 같이 N-IDS와 VAS의 탐지정보를 수집하는 모듈, 이들 정보를 이용한 자산 취약점-위협 상관분석 모듈, 자산 가용성 분석 모듈, 네트워크 취약점-위협 상관분석 모듈 및 시스템 관리를 위한 어드민 콘솔(Admin Console)로 구성된다. 자산 취약점-위협 상관분석 모듈에서는 발생한 위협이 자산의 잔류 취약점과 상관관계가

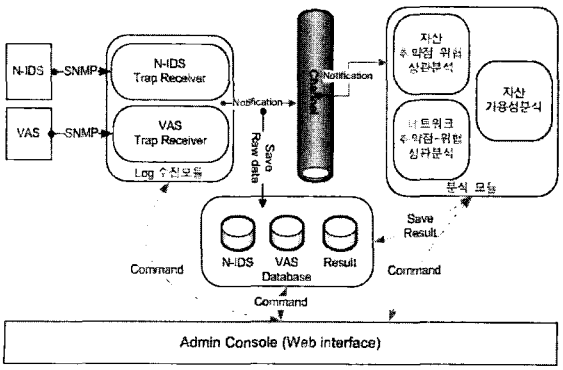


그림 4. N-IDS 조기경보 시스템 구성도

OID	Object Name	Type	Description
1.3.6.1.4.1.10765.2.1.1	nwMessageId	Integer	Trap 메시지에 대한 식별 ID
1.3.6.1.4.1.10765.2.1.2	nwEventGroupId	Integer	발생한 이벤트가 속한 그룹 ID :: 동일한 IDE가 여러 번 발생할 경우, NeoWatcher에ESM에서는 매번 전송하는 것이 아니라, 로그 수집 정책에 따라 일련의 묶음으로 만들 시스템에 전송합니다. 여기서, 이 오브젝트는 각 묶음을 식별하기 위한 역할입니다.
1.3.6.1.4.1.10765.2.1.3	nwEventCount	Integer	해당 이벤트가 발생한 횟수 :: IDE 그룹에 포함된 IDE의 개수를 나타 냅니다.
1.3.6.1.4.1.10765.2.1.4	nwFirstEventTime	DateAndTime	이벤트 그룹과 관련된 IDE의 최초 발생 시간입니다.
1.3.6.1.4.1.10765.2.1.5	nwDetectionTime	DateAndTime	IDE 그룹에 포함된 침입을 중 가장 마지막에 포함된 IDE의 시간을 나타냅니다.
1.3.6.1.4.1.10765.2.1.6	nwRuleGroup	String	관련 침입 탐지 룰이 포함된 룰 그룹을 나타 냅니다.
1.3.6.1.4.1.10765.2.1.7	nwRule	String	해킹이나 해킹 시도 등의 네트워크 침입을 탐지하기 위한 규칙
1.3.6.1.4.1.10765.2.1.8	nwSeverity	Integer	발생한 이벤트의 위협도
1.3.6.1.4.1.10765.2.1.9	nwService	Integer	패킷에 제공된 서비스(웹킷, ftp 등등)
1.3.6.1.4.1.10765.2.1.10	nwProtocol	String	TCP, UDP, SNMP, ARP 같은 프로토콜을 종류를 나타냅니다. 상황하면, 침입자가 침입 대상 서비스에 어떤 베이스 프로토콜을 접근 했는지를 나타 냅니다. (ex : DNS 서비스의 경우, UDP 혹은 TCP로 접근 가능합니다.)
1.3.6.1.4.1.10765.2.1.11	nwCommType	Integer	서버와 클라이언트가 서로 로컬적 연결되었는지 리모트로 연결되었는지 여부
1.3.6.1.4.1.10765.2.1.12	nwAdapterIndex	Integer	패킷을 잡는 NIC의 index
1.3.6.1.4.1.10765.2.1.13	nwClientMac	Mac Address	침입 자의 MAC address
1.3.6.1.4.1.10765.2.1.14	nwClientIp	IP Address	침입 자의 IP Address
1.3.6.1.4.1.10765.2.1.15	nwClientPort	Integer	침입 자의 Port
1.3.6.1.4.1.10765.2.1.16	nwClientName	String	침입 자의 Host Name
1.3.6.1.4.1.10765.2.1.17	nwServerMac	Mac Address	Victim의 MAC address
1.3.6.1.4.1.10765.2.1.18	nwServerIp	IP Address	Victim의 IP Address
1.3.6.1.4.1.10765.2.1.19	nwServerPort	Integer	Victim의 Port
1.3.6.1.4.1.10765.2.1.20	nwServerName	String	Victim의 Host Name
1.3.6.1.4.1.10765.2.1.21	nwUserName	String	서비스 중 로그인시 필요한 사용자 이름
1.3.6.1.4.1.10765.2.1.22	nwResponse	Integer	대응 종류(Dock, Mail, SMS 등)
1.3.6.1.4.1.10765.2.1.23	nwIntrusionContent	String	침입내용
1.3.6.1.4.1.10765.2.1.24	nwCVE	String	CVE(Common Vulnerabilities and Exposures) Index사에서 정의한 일반적으로 잘 알려진 보안 취약점과 노출 리스트에 대한 식별 번호

그림 5. N-IDS 침입탐지 경보 로그 형식

있는지 분석하고, 자산 가용성 분석 모듈에서는 자산의 잔류 취약점과 무관한 N-IDS로그를 기반으로 위협수준을 산출하여 위험발생 가능성을 진단하며, 네트워크 취약점-위협 상관분석 모듈에서는 네트워크 위험도를 기반으로 네트워크 자산 전체에 대한 위험발생 가능성을 분석한다. 또한 시스템의 모든 프로세스 및 DB 상태를 모니터링하고 통제를 할 수 있도록 하기 위한 어드민 콘솔이 있다.

3. 로그 수집 모듈

N-IDS와 VAS가 제공하는 위협 및 취약점 탐지정보는 SNMP trap으로 데이터를 가져와 외부 DB에 저장한다. 네트워크에 위험을 일으키는 요인은 다양하게 있으나, N-IDS와 VAS로 측정할 수 없는 것은 본 논문에서 고려하지 않는다. 실제 N-IDS 로그 포맷은 [그림 5]와 같은 필드들로 구성된다. SNMP 프로토콜 형태로 구성이 되며, 발생한 침입정보의 각 필드마다 정보 추출을 위한 OID(object ID)와 해당되는 값이 쌍을 이루며 저장되어 있다.[19] 이러한 N-IDS 침입탐지경보 정보는 표준포맷이 설정되어 있지 않기 때문에 제품마다 약간씩 차이가 있다. 따라서 본 논문에서는 N-IDS 로그 정보 중 분석에 필요한 필드 값만을 선택하여 저장한다.

VAS는 자체의 공격코드 DB를 이용하여 자산에 직접 공격시도를 한 후 되돌아오는 정보를 분석하여 취약점 존재를 추정한다. 분석 결과(시스템 OS, 취약점 포트, 프로토콜 취약점 등)는 VAS 자체 DB에 저장이 되고 SNMP형식으로 재구성되어 로그 수집 모듈로 전달된다.

로그 수집 모듈에서는 발생된 N-IDS와 VAS의 로

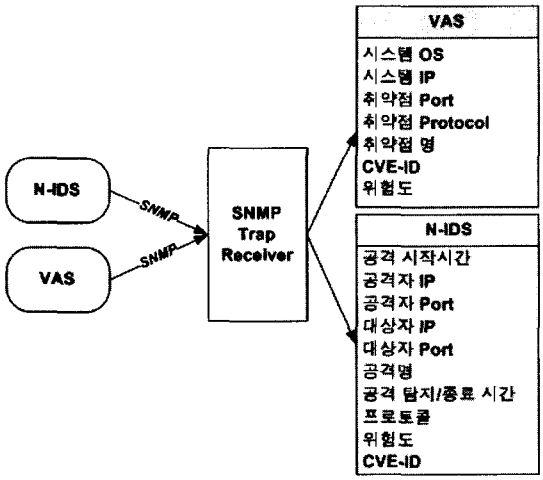


그림 6. 로그 수집 모듈 구성도

그정보 중에서 분석에 필요한 데이터만 선별하여 [그림 6]과 같이 각각 사전 정의한 형태의 DB로 재구성하여 저장한다. IP 주소와 CVE-ID(Common Vulnerability Exposure-ID)[20] 정보는 N-IDS와 VAS DB간의 데이터 상관 분석시 중요한 key값으로 활용된다.

4. 자산 취약점-위협 상관분석

자산에 내재한 취약점의 존재는 잠재적인 위협을 현실화할 수 있는 역할을 하며, 특정한 취약점에 대해 다수의 위협이 상관된다. 현재 많은 N-IDS들은 관리대상 네트워크의 자산이 가진 취약점과 무관한 위협을 다수 탐지하여 보안 관리자의 부담을 가중시키고 있다. N-IDS 로그를 VAS로그와 상관시키면, 자산의 취약점을 이용하여 위협을 발생시킬 수 있는 위협만을 찾아낼 수 있다. 또한, N-IDS의 문제점으로 지적되는 탐지오류를 줄일 수 있어 운용자의 관리 부담을 감소시킬 수 있다[17-18].

[그림 7]은 VAS가 탐지한 특정 취약점에 대해 N-IDS의 로그가 상관되는 형태를 보인 것이다. 동일 IP에 대한 N-IDS 로그의 CVE-ID가 VAS로그에 있는 CVE-ID와 일치된다면, 이는 자산이 가지고 있는 취약점을 공격하는 것이므로 해당 자산에 직접적인 피해 유발이 가능하다. 따라서 이러한 형태의 N-IDS 로그 발생시 경보수준이 가장 높은 Critical 경보를 신속하게 발생시켜 보안 관리자가 즉각적인 대응을 할 수 있도록 해야 한다. 발생되는 모든 N-IDS로그 정보를 VAS 로그와 대조하며 취약점을 공격하는 위협

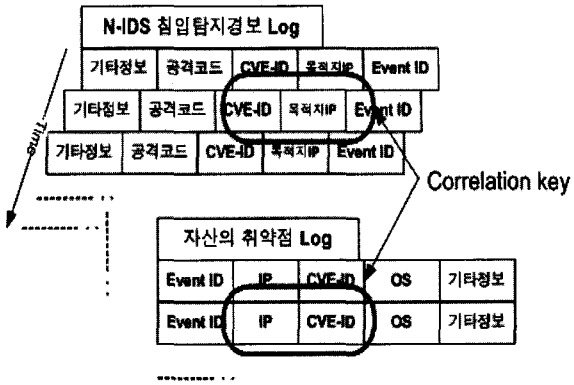


그림 7. 취약점-위협 상관성 분석

이 발생하였는지를 지속적으로 판단한다.

5. 자산 가용성 분석

앞 절에서 언급한 바와 같이 자산이 가진 취약점을 공격하지 않은 위협들은 직접적으로 자산에 피해를 줄 가능성은 희박하다. 그러나 반복적이고 지속적인 공격은 자산 자체의 가용성 저하를 초래할 수 있다. 기존의 N-IDS들은 자산이 가진 취약점과 상관성이 없는 위협들에 대해서도 단순히 발생순서에 따라 경보를 생성함으로써 보안 관리자의 부담을 가중 시키고 있다.

이러한 문제를 해결하기 위해 본 논문에서는 N-IDS의 로그 중 자산의 취약점을 공격한 것을 제외한 나머지 위협로그를 이용하여 단위 시간 동안 위협수준을 판단하고 그 수준에 따라 새로운 경보를 생성한다. 또한, 대부분의 위협은 발신지 주소를 변조하여 이루어지므로, 본 논문에서는 위협을 받고 있는 자산별로 일정 시간 동안 발생하는 위협패턴을 하나의 DB 레코드로 관리함으로써 위험발생 가능성이 있는 자산의 식별과 위험 가능성을 효과적으로 인식할 수 있는 방법을 제안한다.

[그림 8]은 자산 가용성 분석을 위한 알고리즘이다. 먼저 취약점-위협 상관분석 후 취약점과 무관한 N-IDS 로그를 순차적으로 위협대상 자산 별로 DB 레코드를 생성하고, 단위 시간 동안 발생하는 위협의 횟수와 유형을 추가해 나간다. 이때 위협유형 정보는 공격시간, 공격자 IP, 공격 대상 포트 등의 정보를 포함하며 특정 자산에 새로운 위협이 발생할 때마다 시간단위 동안 순차적으로 동일 DB 레코드에 추가하여 기록해 나간다. 이러한 정보를 기반으로 위협수준을 분석하고 수준에 따른 경보를 생성한다.

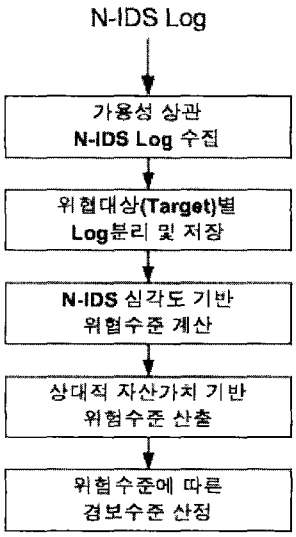


그림 8. 자산 가용성 분석

5.1 위협 수준 산정

N-IDS는 탐지한 개별 위협의 속성에 따라 미리 설정된 위험도(risk) 정보를 갖고 있다. 본 논문에서 사용한 N-IDS 위험도는 4단계로 나누어지며 다음과 같은 수치로 매핑 된다.

- 1 = Low
- 2 = Medium
- 3 = High
- 4 = Very High

따라서 본 논문에서는 특정 자산에 대한 위협의 빈도와 개별 위협에 대해 N-IDS에서 설정한 위험도 정보를 이용하여 자산에 대한 위협수준(T)을 산정한다.

$$T = \sum_{i=1}^{n} R_i$$

(n: 단위 시간 동안 발생한 위협수, R_i : i 번째 위협의 위험도)

위 식에서 단위시간(사전 설정된 time window, 1시간 미만에서 네트워크 특성에 따라 임의 설정) 동안 산정된 위협수준의 누적 값이 일정치 이상 되면 위협대상 자산의 가용성에 문제가 발생할 수 있다고 판단한다.

5.2 경보 발령 수준 결정

특정 자산들에 대한 위협이 일정수준(임계치)을 넘을 경우, 단위시간 동안 발생한 위협의 위험도 합을 기반으로 경보수준을 산정한다. 일반적으로 경보의 수준은 4단계(Critical, Major, Minor 및 Warning)로 구분하며, 각 단계의 구분을 위한 임계값(Threshold)은 과거 1시간 전의 위협수준을 기준 값으로 설정한다. 경보발령 수준은 [그림 9]와 같은 알고리즘을 이용하여 결정한다. 발생한 N-IDS 로그가 현재 자산이 가지고 있는 취약점과 상관성이 존재하는지 파악을 한다. 만약에 취약점과의 상관성이 존재한다면 경보 수준이 가장 높은 Critical경보를 발생하여 즉각 보안 관리자가 대처할 수 있도록 한다. 그러나 취약점과의 상관성이 존재하지 않는다면 단위시간 동안의 위협수준 값을 지난 1시간 동안의 평균 위협 수준과 비교한다. 만약 현재의 위협수준 값이 지난 1시간 전의 위협수준보다 크게 된다면 다음과 같은 기준에 의해 해당 경보를 발생시킨다.

- 1 ~ 2배: Warning
- 2 ~ 3배: Minor
- 3 ~ 4배: Major
- 4배 이상: Critical

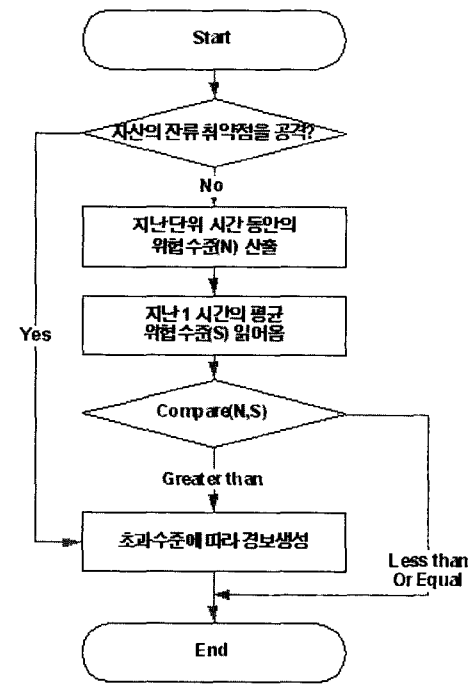


그림 9. 자산 가용성 경보 발령 수준 결정 알고리즘

6. 네트워크 취약점-위협 상관분석

4.4 절에서 제안한 자산 취약점-위협 상관분석은 개별 자산에 실질적으로 피해를 줄 수 있는 위협을 판단할 수 있지만 전체 네트워크 대상의 위협을 탐지하기에는 적합하지 못하다.

이 절에서 제안하는 네트워크 위험 조기 경보 생성 알고리즘은 네트워크 전체적인 위협 중에서 실제 네트워크 내부 자산에 영향을 주는 위협의 비율을 통해 위험도를 산정하고, 위험도가 특정 임계치를 넘는지 여부를 통해 경보를 생성한다. 이 임계치는 네트워크 트래픽/위협/취약점 현황과 위험 관리 정책에 따라 결정된다.

네트워크 취약점-위협 상관분석을 위한 알고리즘은 다음과 같다. 전체 자산의 수를 $TotalAsset$이라 하고, i번째 자산의 가치를 AV_i라 하며, i번째 자산에 대한 N-IDS 로그들 중 j번째 로그의 위험도를 $T_i[j]$라 한다. i번째 자산에 대한 N-IDS 로그 전체의 인덱스 집합을 F_i라 하고, VAS로그와의 상관 분석을 통해 실제 취약점과 연관이 있다고 파악된 로그들의 인덱스 집합을 B_i라고 한다.

예를 들어 2번째 자산으로 향하는 N-IDS 로그가 10개가 있고, 그 중에서 8번째와 10번째 로그가 실제 취약점과 연관이 있다면 $B_2=\{8, 10\}$이 된다. 이 때 네트워크 위험도(R_N)를 계산하기 위한 식은 다음과 같다.

$$R_N = \frac{\sum_{i=1}^{TotalAsset}\left(\frac{\sum_{k\in B_i} T_i[k]}{\sum_{j\in F_i} T_i[j]} \times AV_i\right)}{\sum_{i=1}^{TotalAsset} AV_i}(\%) \qquad (1)$$

식 (1)에서 $\sum_{j\in F_i} T_i[j]$는 i번째 자산으로 향하는 모든 위협의 위험도 합을 의미한다. 이 값은 현재 i번째 자산이 받고 있는 위협의 전체 크기를 정량화한 것이다.

$\sum_{k\in B_i} T_i[k]$는 i번째 자산으로 향하는 모든 위협중 실제 i번째 자산에 영향을 줄 수 있는 위협의 위험도 합을 의미한다.

실제 위협을 줄 수 있는지 여부를 판단하는 기준은 4.4절에서 설명한 N-IDS로그와 VAS 로그와의 상관관계 분석 기법을 이용한다.

$\frac{\sum_{k\in B_i} T_i[k]}{\sum_{j\in F_i} T_i[j]}$는 i번째 자산으로 들어오는 전체 위협 중에서 i번째 자산에 영향을 줄 수 있는 위협의 비율이다. $\left(\frac{\sum_{k\in B_i} T_i[k]}{\sum_{j\in F_i} T_i[j]} \times AV_i\right)$는 $\frac{\sum_{k\in B_i} T_i[k]}{\sum_{j\in F_i} T_i[j]}$에 i번째 자산의 가치를 곱한 값으로 자산의 가치에 따라 위험의 크기를 다르게 하는 역할을 한다.

이 값을 모든 자산에 대하여 더한 뒤 $\sum_{i=1}^{TotalAsset} AV_i$, 즉 전체 자산 가치의 합으로 나누면 자산의 가치를 반영한 네트워크 위험도를 얻을 수 있다.

이러한 정량화된 네트워크 위험도를 기반으로 관리 대상 네트워크의 위험상황을 신속하게 탐지하여 보안 정책에 따라 즉각적인 행동을 취할 수 있도록 한다.

V. 결 론

지난 2003년 1월 25일 인터넷 대란 이후 많은 기업들이 네트워크를 통해 유통되는 비정상 트래픽을 감시, 차단하기 위해 다양한 보안장비들을 도입, 운용하는데 많은 비용을 쓰고 있다. 하지만, 각종 보안장비들이 제공하는 대량의 탐지정보들 간에 존재하는 상관성들을 분석하고, 가공하는 작업은 여전히 보안 관리자의 직관과 수작업에 많이 의존하고 있어 신속한 대응에는 현실적인 제약이 있다.

본 논문에서는 이와 같은 문제를 해결하기 위해 네트워크에서 실시간 위협탐지를 위해 사용되는 N-IDS와 정기적인 보안감사용으로 운영되는 VAS를 연동하여 네트워크의 조기 경보 시스템을 설계하는 방법을 제시하였다. VAS의 취약점 탐지정보와 N-IDS의 위협 탐지정보간 상관속성을 이용하면 자산에 발생할 수 있는 위험의 유형에 따라 대응방안을 결정할 수 있게 된다.

네트워크에서 개별적으로 운용하던 N-IDS와 VAS를 이용함으로써 기존의 다른 상용 조기 경보 시스템보다 구축에 따른 비용대비 효과가 높고, 위협과 취약점의 탐지기능을 독자적으로 진화, 발전시킬 수 있어 시스템의 확장성과 유연성에 장점을 갖는다.

향후, 효과적인 기능 확장을 위해서는 표준 전달 데이터 포맷인 IDMEF(Intrusion Detection Message Exchange Format)에 대한 적용 연구, 위협경보의 최적화를 위해 타 보안시스템 로그와의 상관성 분석 및 위협경보의 단계구분을 위한 기준치 설정방법 등에 대한 추가적인 연구가 필요하다.

참 고 문 헌

[1] Symantec , "Report on internet security threat", 2004

[2] Nicholas C Weaver, "Warhol worms: The potential for very fast internet plagues", 2002.

[3] Abor Networks, "A Snapshot of Global Internet Worm Activity", Nov. 2001.

[4] Gatner, "IDS a failure, firewalls recommanded", Web Host Industry Review, June 11.

[5] 권기훈 외 4명, "트래픽 분석에 의한 광대역 네트워크 조기 경보 기법", 한국정보보호학회지, 제14권, 제4호, pp.111-120, 2004년 8월

[6] 정재훈 2명, "인터넷 트래픽 수동적 측정 도구 Cflowd의 설치 및 설정방법", IPv6 포럼 코리아 기술문서2001-006, 2001

[7] R. Jain and S.A. Routhier, "Packet Trains-Measurements and a New Model for Computer Network Traffic", IEEE JSAC, Sep. 1986

[8] NetFlow, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/netlct/tech/napps_wp.htm

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

[10] Honeynet Project, "Know Your Enemy: Honeynets", http://project.honeynet.org/papers/honeynet/

[11] Snort, http://www.snort.org

[12] Symantec, "Symantec Decoy Server", http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=157

[13] 한국전산원, 위험분석 방법론 및 자동화 도구 기술 이전 교육 교재.

[14] 최상수 외 3명, "보안관리 및 위험분석을 위한 분류체계, 평가기준 및 평가스케일의 조사연구", 한국정보보호학회지, 13권 제 3호, pp. 38-49, 2003년 6월.

[15] 한국정보보호진흥원, "취약점 분석, 평가를 위한 자산분석 지침(안)", 2001년 9월

[16] Edward G. Amoroso, "Fundamentals of Computer Security Technology", AT&T Bell Lab.

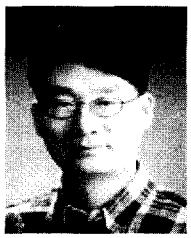
[17] 문호건, 최진기, "네트워크의 자산, 취약점 및 위협의 상관성을 이용한 N-IDS Log 최적화 시스템 설계," CISC-W'03 Proceedings, pp. 153-159, 2003년 12월

[18] 문호건, 최진기, "실시간 네트워크 위험분석 시스템의 설계 및 분석", JCCI2004, 2004년 4월

[19] 윈스테크넷, "Sniper 3.0 관리자 설명서", 2004

[20] ICAT Vulnerability Information Service, http://icat.nist.gov/icat.cfm.

〈著 者 紹 介〉

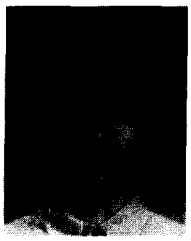


문 호 건 (Ho-Kun Moon)
정회원

1985년 : 숭실대학교 전자공학과 졸업(학사)
1987년 : 중앙대학교 전자공학과 졸업(석사)
2005년 : 부산대학교 전자공학과 졸업(박사)
1987년~2004년 : KT 차세대 통신망연구소 보안기술연구실장
2005년~현재 : KT 정보보호단 기술개발 1부장
〈관심분야〉 위험분석, 위험관리, 네트워크 보안

최 진 기 (Jin-gi Choe)

1998년 : 숭실대학교 전자공학과 (학사)
1999년~2004년 : KT 차세대통신망연구소 보안기술연구실
2005년 : 충남대학교 정보통신공학과(석사)
2005년~현재 : KT 정보보호단 기술개발1부
〈관심분야〉 위험분석, 네트워크 보안



강 유 (Yu Kang)

2003년: 서울대학교 컴퓨터공학과 (학사)
2004년~현재 : KT 정보보호단 기술개발 1부
〈관심분야〉 모의해킹, 위험분석, 컴퓨터 포렌식

이 명 수 (Myung-soo Rhee)

1989년 : 연세대학교 대학원 전자공학과 박사과정 졸업
1990년~2004년 : KT 네트워크 보안연구팀장
2005년 : KT 정보보호기술팀장
2004년~2005년 : 정보보호학회 무임소이사
〈관심분야〉 e-business, 플랫폼 business, 네트워크 컴퓨팅, 프라이버시 보호