정책기반 네트워크 보안 관리

Network Security Management Based on Policy Management

이수형(S.H. Lee) 능동보안기술연구팀 선임연구원
김진오(J.O. Kim) 능동보안기술연구팀 선임연구원
장범환(B.H. Chang) 능동보안기술연구팀 선임연구원
나중찬(J.C. Na) 능동보안기술연구팀 책임연구원, 팀장

기존의 사이버 공격은 특정 호스트나 서버를 목표로 하여 정보의 탈취 및 변경 등에 집중되었으나, 현재는 직접 혹은 간접적으로 과다 트래픽을 유발하여 네트워크 서비스를 마비시키는 방향으로 그 경향이 변하고 있다. 이런 사이버 공격을 방지하여 네트워크의 안정적인 서비스의 제공을 위해서는 공격 징후나 이상 징후를 탐지하고 네트워크 차원에서 이에 대한 대응 방안을 결정하여 이를 네트워크 상에 강제할 수 있는 체계적인 보안 관리가 이루어져야 한다. 또한 네트워크 각 운용 주체별로 개별 보안 상황에 대해 적용할 보안 정책이 다르므로 이를 모델링하고 적용할 수 있는 방법이 제공되어야 한다. 본 논문에서는 정책 기반 네트워크 보안 관리 기능을 수행하기 위해 필요한 공격 및 이상 징후의 탐지, 그에 대한 대응과 이런 일련의 작업에 보안 정책을 강제하기 위한 보안 정책관련 연구 동향에 대해 다루도록 한다.

I. 서 론

인터넷의 급격한 확산과 인터넷을 이용하는 응용의 수가 급격히 증가함에 따라 인터넷 상에서 이루어지는 사이버 공격의 발생 빈도는 점점 증가하고 있으며, 이로 인해 입게 되는 시간적·경제적 피해 규모는 이전과는 비교할 수 없을 정도로 커지고 있다. 또한 공격 수준을 보면 기존의 가입자 단에 위치하는 시스템들을 목표로 하는 공격에서 1.25 인터넷 침해 사고에서처럼 네트워크 자체의 운용이나 성능에 영향을 미치고 결과적으로는 네트워크 서비스 제공 자체를 위협하는 단계에 이르렀다.

네트워크 보안의 궁극적인 목적은 사용자들이 네트워크를 이용하여 제공되는 각 서비스들을 어떤 상황에서도 안정적이고 안전하게 이용할 수 있도록 보장하는 데 있다고 할 수 있다, 이를 위해서는 각 응용 서비스를 구현하고 제공하는 서버 및 응용 프로그램에 대한 보호와 각 서버와 사용자 상호간의 데이터 교환을 담당하는 네트워크의 보호가 확보되어야 한다. 또한 공격이나 보안상 침해 요인이 발생하였을 경우 이에 대한 대응 방안이 강구되어 네트워크 상에 실행됨으로써 해당 공격이나 침해 요인으로 인해 발생하게 될 부정적 효과를 차단 또는 완화할 수 있어야 한다.

이와 같은 보안과 관련된 일련의 작업을 결정하고 수행하는 과정에는 네트워크나 응용 서비스의 각 운용 주체에 고유한 보안 정책이 존재하고 이를 반영할 수 있어야 한다. 즉 공격이나 이상 징후를 탐지함에 있어서는 해당 운용 도메인 상에서 발생하는 보안 관련 이벤트 중 어떤 것들을 집중적으로 모니터링하고 이들 이벤트에 대해서 어떤 분석 방법을 적용하여 공격이나 이상징후를 탐지할 것인지, 또한 탐지된 공격 및 이상 징후를 어떻게 네트워크 수준의 침해 요소로 분석하여 전체적인 네트워크 보안 상황을 판단할 것인지는 각 운용 도메인별로 달라질 수 밖에 없다. 또한 해당 보안 상황에 대한 대응을 수행함에 있어 어디에 어떤 대응 메커니즘을 수행할 것인지도 각 도메인별 네트워크 구성, 주된 제공 서

비스에 따라 달라질 수 밖에 없고 이런 요소들이 모두 보안 관련 정책이라 할 수 있다.

정책 기반의 네트워크 보안 관리는 위에서 기술된 바와 같이 보안 관련 이벤트 모니터링, 수집하여 이를 분석하고 이를 이용한 공격 및 이상 징후의 탐지 및 대응에 이르는 일련의 보안 행위에 있어 해당 도메인이 추구하는 보안 정책을 강제하여 수행할 수 있도록 관련 기능을 제공하는 보안 프레임워크이다.

본 논문에서는 정책기반의 네트워크 보안 관리를 위해 필요한 요소 기술의 연구 동향과 필요에 따라 현재 당 팀에서 연구중인 보안관리시스템과 관련된 내용을 기술하도록 한다. 이를 위해서 우선 네트워크 보안을 위협하는 침해 요소에 대한 현재의 동향에 대해서 언급하고, 이들 침해 요소로부터 현재의 보안 상황을 파악하기 위한 분석 방법에 대해 다루도록 한다. 이후 분석된 결과에 따라 네트워크의 안정성을 확보하기 위해 취할 수 있는 대응 방안에 대해서 기술하고, 각 단계별로 해당 도메인의 보안 정책을 강제하기 위한 보안 정책관련 연구동향에 대해 언급한 후 결론을 짓도록 한다.

Ⅱ. 네트워크 침해 요소의 변화 추세

네트워크 침해 유형의 큰 변화는 예전의 특정 개별 시스템이나 해당 시스템이 제공하는 서비스에 대한 공격에서 백본 네트워크 수준의 네트워크에 대한 공격으로 변화하고 있다는 점이다.

즉, 초기의 공격 형태는 정보의 탈취나 변경을 목적으로 특정 서버에 침입하거나 특정 서버에 침입하기 위한 사전 공격 형태로써 LAN(Local Area Network) 수준의 네트워크 상에 존재하는 호스트 및 제공 서비스 등에 대한 정보를 획득하는 공격이었다. 이후 DDoS(Distributed Denial of Service) 공격처럼 특정 서버의 동작을 방해함으로써 해당 서비스의 제공을 방해하는 공격이 주를 이루었다. 이런 공격의 경우 특정 서버나 해당 서버에서 제공하는 서비스 입장에서 보면 그 피해가 크다고 할 수 있으나 그 피해의 범위는 특정 서버나 해당 서버가 존재하는 로컬 네트워크 수준을 넘어서지 않아 광역 네트워크를 통하여 제공되는 타 서비스에 미치는 영향은 거의 없는 것이 그 특징이다.

반면 요즘 공격의 주요 형태는 광역 네트워크 자체(즉 네트워크를 구성하는 장비나 네트워크 운용 메커니즘)에 대한 공격이 이루어지거나, 공격의 부수적인 효과로써 광역 네트워크의 서비스 제공을 방해한다는 점이다. 그 예로써 2003년에 발생한 1.25 인터넷 침해사고를 들 수 있다. 이 때 실제 공격은 SQL 슬래머라는 인터넷 웜의 단시간 내 기하 급수적인 확산이었고 이와 더불어 네트워크 상에 과다 트래픽의 증가가 있었다. 하지만 실제 네트워크 서비스 마비를 유발한 것은 웜의 확산에 필요한 DNS(Domain Name Service) 서버에 대한 질의가 단시간 내 과도하게 집중된 것이 그 원인으로 보고되고 있다[1]. 이는 네트워크 서비스 마비라는 초유의 사태가 웜 전파라는 공격의 직접적인 부수적인 효과로 발생한 것이라 볼 수 있다. 현재 발생하고 있는 공격의 특징은 다음과 같다.

• 피해 전파 속도의 신속성

1.25 사고의 경우처럼 수 분~수십 분 내에 전세계 네트워크를 대상으로 공격이 가능하고 이론적인 분석상 3분 내에 공격의 전파 및 네트워크 마비가 가능한 것으로 보고되고 있다[2],[3]. 이럴 경우 기존의 보안 관리 프레임워크에서처럼 관리자가 보안 시스템으로부터 발생하는 경보 이벤트를 분석하고 이를 바탕으로 수동 대응하여 공격을 처리하기는 어렵다.

• Zero-Day 공격의 증가

1.25 사고때도 Slammer 웜은 알려진 공격이었지만 그 부수적인 영향으로 네트워크가 마비되는 것은 예상하지 못한 결과이다. 더욱이 요즘은 새로운 취약점이 발표되면 이를 이용한 공격을 제작하는 데 2일 정도 소요되는 것으로 예상하고 있다. 이런 경우 기존 시그니처 기반의 공격 탐지 기법을 이용하여 이를 처리하기는 어려울 것으로 예상된다.

• 범위의 광역화 및 분산화

그 범위가 특정 서버나 로컬 네트워크 수준이 아

니라 전체 광역망에 영향을 미치고 해당 광역망을 이용하여 제공되는 모든 서비스에 피해를 입히게 된다. 또한 웜 전파의 경우처럼 네트워크 상에 그 영향이 나타나기 시작하는 시점에서는 그 공격이나 침해 요인의 원천이 특정 지점이나 서버에 국한되는 것이 아니라 광역 네트워크 내의 여러 곳이 분산되어 나타나고 그 영향은 네트워크 전체에 미친다는 점이다.

Ⅲ. 네트워크 보안 상황의 분석

네트워크의 보안 상황을 파악하기 위한 방법으로는 기존의 보안 시스템으로부터 발생하는 보안 관련 경보 이벤트를 이용하는 방법과 네트워크 상에 존재하는 트래픽의 변화를 분석하는 방법이 있을 수 있다.

기존 보안 시스템의 경우 특정 공격 유형의 특징을 모델링하여 이를 시그니처화하고 이를 바탕으로 특정 공격을 탐지하게 된다. 이럴 경우 기존의 알려진 공격이 이루어질 경우 이에 대한 탐지의 정확성은 높으나 Zero-Day Attack과 같은 전혀 새로운 공격을 탐지하는 것은 어렵고, 시그니처라는 특정 패턴을 바탕으로 탐지하기 때문에 다량의 경보가 발생하게 된다. 특히 네트워크 수준의 공격 상황에 대한 분석이 이루어질 경우 다수의 보안 장비로부터 발생하는 수많은 경보 이벤트를 어떻게 통합하여 분석할 것인가에 대한 방안이 강구되어야 한다.

트래픽 분석의 경우 네트워크의 성능을 저하시킬 정도의 과다 이상 트래픽을 탐지하기 위한 것으로 새로운 웜이나 1.25 사고때처럼 알려지지 않은 부수적인 효과로써 다량의 트래픽을 유발하는 침해 요인 탐지에 효과적이다.

1. 경보 연관성 분석을 통한 공격 상황 분석

네트워크 내 다수의 보안 장비로부터 발생하는 대량의 경보를 통합하여 분석함으로써 네트워크 전체의 보안 상황을 파악하기 위해서는 보안 경보 상호 간의 연관성 분석을 통한 경보의 중복성, 순차성, 전체 상황 분석이 이루어져야 한다.

가. 연관성 분석의 정의

보안 경보의 연관성 분석은 다양한 보안 장비에서 발생하는 보안경보간의 상호 연관관계를 통하여 보안 위협을 보다 정확하게 식별하는 것을 의미하고 그 분석 과정은 (그림 1)과 같다.

• 보안경보 수집

네트워크 내의 다수의 지점에 존재하는 이기종의 보안장비로부터 보안경보를 수집한다. 보안경보 수집은 네트워크의 규모나 서비스의 규모와 관계없이 보안경보의 유실됨이 없이 수집해야 하며, 각 보안 장비 제조회사에 따라 다양한 인터페이스를 제공해야 한다. 현존하는 인터페이스로는 syslog, API (Application Programming Interface), IDXP(Intrusion Detection eXchange Protocol), SNMP (Simple Network Management Protocol) Trap, text file, Cisco IDS RDEP(Remote Data Exchange Protocol) 등이 있다.

• 보안경보 필터링

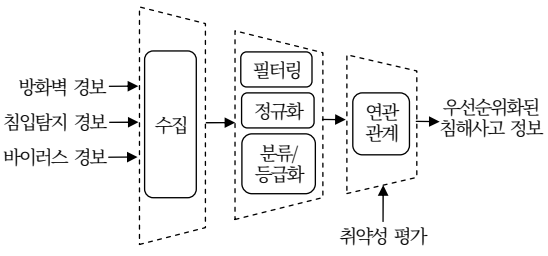
보안위협을 나타내지 않는 보안경보는 제거함으로써 연관성 분석 시간을 줄인다.

• 보안경보 정규화

다양한 형식으로 수집되는 보안경보 속성 표현의 일관성을 유지하기 위해 형식 정규화를 수행한다. 침입탐지 경보인 경우에는 연관성 분석을 위한 명칭 및 심각도 표현에 대한 통일성을 제공한다.

• 보안경보 분류 및 등급화

반복적인 공격으로 인한 중복된 보안경보를 축약하고, 하나의 공격에 대해 여러 개의 불필요한 중복



(그림 1) 보안 경보의 연관성 분석 과정

된 보안경보를 제거한다. 또한 보안경보의 공통적인 특징을 분석하여 각 보안경보를 분류한다. 또한 자산가치에 따라 보안경보 등급을 부여한다.

나. 연구 분야

보안경보 간의 연관성 분석 분야는 주로 중복성(duplication), 순차성(consequence), 상황(situation) 등과 관련하여 연구가 수행되어 왔다[4].

• 중복성 분석

중복성 분석은 반복적인 공격에 의해 보안경보가 반복적으로 발생하는 것을 탐지하거나, 또는 단일 공격에 의한 중복된 보안경보 발생을 탐지하는 기능을 수행한다. 전자의 경우는 중복된 보안경보를 축약 처리하여 분석 작업의 부하를 감소시키며, 경우에 따라서는 심각도를 높여 보안경보에 대한 위협을 우선적으로 처리할 수 있도록 이용할 수 있다. 후자의 경우는 불필요한 보안경보를 제거하여 분석 작업의 부하를 감소시키는 데 이용될 수 있다.

• 순차성 분석

어떤 공격들은 해당 공격 수행에 있어 적어도 몇 개의 보안경보 생성을 수반하며, 이러한 보안경보는 주어진 시간 구간에서 순차적인 패턴을 이룰 수 있다. 순차성 분석은 보안경보의 순차성 패턴을 탐지하는 기능을 수행한다. 이는 특정 공격 진위 여부의 파악이 가능하며, 다음 공격 행위의 예측을 시도할 수 있으며, 보안경보의 오탐 여부 판단에 이용될 수 있고, 또한 순차적인 패턴 체인에 누락된 경보에 대해서 해당 보안장비의 동작여부에 대한 검사가 가능함을 의미한다.

• 상황 분석

상황 분석은 네트워크 상에서 발생하는 수천에서 수백만 개의 보안경보에 대해 공통적인 특징에 따라 몇 가지 상태 집합으로 분류함으로써 네트워크 공격 유형 정보를 생성한다. 이는 곧 네트워크 보안관점의 직관적인 공격상황 정보를 제시함을 의미한다. 또한 단일 보안경보는 중요하지 않을 수 있으나, 반복적으로 발생하는 보안경보는 심각할 수 있다.

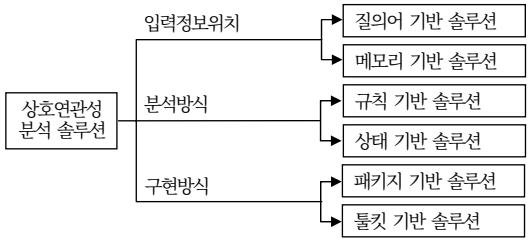
다. 연관성 분석 솔류션 유형

보안경보의 상호 연관성 분석 솔루션은 (그림 2)와 같이 상호연관성의 입력 정보의 위치, 상호연관성 분석 방식, 구현 방식에 따라 분류된다.

질의어(SQL) 기반의 솔루션은 보안장비로부터 발생된 보안경보를 데이터베이스에 저장한 후, 연관성 분석 이전에 질의어를 통해 보안경보를 메인 메모리에 적재하여 수행한다. 일반적으로 보안경보 데이터 베이스를 디스크에 두고 사용함으로써 과도한 디스크 입출력으로 인하여 본질적인 성능에 한계를 보인다. 메모리 기반의 솔루션은 연관성 분석 수행과 함께 병렬적으로 보안경보를 저장한다. 메모리 기반의 솔루션은 빠르며 효과적이다.

규칙 기반 솔루션은 특정한 보안경보의 순차성 패턴을 탐지하여 공격의 진위 여부의 파악을 수행한다. 이 접근 방법은 잘 알려진 패턴에 대해서는 탐지율이 높기 때문에 많은 제품들이 이 접근방법을 사용하고 있으나, 새로운 공격은 순차성 규칙이 반영되기 이전에는 탐지가 불가능하다는 단점을 갖는다. 또한 규칙들은 시간이 지남에 따라 폭발적으로 증가하는 경향이 있으며, 이로 인하여 규칙들에 대한 상당한 유지보수를 요구한다. 이에 비해 상태 기반 솔루션은 고수준의 추상화한 공격 행위에 해당되는지를 탐지하는 것이다. 이 솔루션의 접근 방법은 구현의 어려움은 가지고 있으나, 관리 비용의 불필요 및 새로운 공격 행위에 대한 탐지가 가능하다.

연관성 분석 솔루션은 제조회사에 의해 사용 가능한 특징으로 제한하는 패키지 기반의 제품과 사용자의 정확한 필요성 환경 및 인프라에 따른 맞춤형이 가능한 툴킷 기반의 제품이 제공되고 있다.



(그림 2) 상호연관성 분석 솔루션 분류

2. 보안 관점에서의 트래픽 분석

트래픽 분석의 주목적은 이상 과다 트래픽을 탐지하여 지속적이고 안정적인 네트워크 서비스를 제공하는 데 있다.

가. 트래픽 분석의 정의

이상 과다 트래픽은 그 트래픽이 공격으로 인해 유발된 것과는 상관없이 현저한 네트워크 성능 저하를 유발함으로써 정상적인 네트워크 서비스를 방해하는 트래픽이라 할 수 있다.

이상 트래픽 탐지 방법은 정상상태의 트래픽을 모델링하여 이에 대한 프로파일을 구축하고 매 시점에서 수집한 트래픽을 이 정상 상태 프로파일과 비교함으로써 그 이상 여부를 판단하는 비정상행위 기반 탐지 방법을 이용한다. 트래픽 분석을 위해 선행적으로 해결되어야 할 부분은 다음과 같다.

• 트래픽 특성 파라미터의 정의

트래픽의 특징을 표현하는 많은 파라미터 중에 어떤 파라미터를 초점을 맞추어 트래픽을 분석할 것인지를 결정하는 것이다. 이를 위해서는 분석 대상 네트워크 상의 트래픽 특성에 대한 이해, 해당 운용 도메인에서의 주된 보안 대상에 대한 정책, 트래픽의 각 특성 파라미터와 공격과의 상호 연관성에 대한 분석이 이루어져야 한다.

• 분석 모델

수집된 트래픽 데이터로부터 정상상태의 트래픽 모델을 프로파일링하고 이를 바탕으로 각 시점에서의 트래픽을 정상 상태 프로파일과 비교하여 이상 여부를 판단하는 기능을 수행한다.

공격 전파 및 그 파급효과의 신속성을 고려할 때 (준) 실시간으로 처리가 가능한 계산량은 정상상태에 대한 모델링의 정확도와 더불어 모델을 개발함에 있어 가장 중요한 고려 요소이다. 사용자 개입이 최소화될 수 있도록 모델 자체적으로 도입 시에는 자체 학습이 가능하고, 운용 시에는 트래픽 변동 특성에 자체 적응이 가능하여야 한다. 다양한 특성 파라미터에 적용될 수 있도록 일반화가 가능하여야 하며, 트래픽 모델링의 정확도와 탐지의 민감도 사이의 적절한 조정이 가능하여야 한다.

• 분석 프레임워크

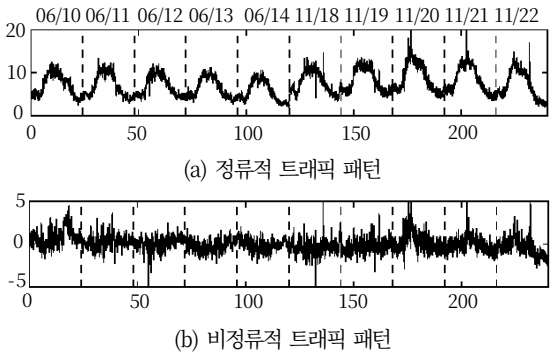
대상 트래픽 특성 파라미터와 분석 모델을 적용하여 전체적인 트래픽 분석의 절차와 구조를 결정짓는 것으로 각 특성 파라미터 분석 결과와 적용 분석 모델별 분석 결과 상호간의 상호 연관성 분석 결과로써 최종적인 결과를 산출하게 된다.

나. 분석 모델에 대한 연구 동향

• 시계열 분석

트래픽의 가장 큰 특징인 시간대별 변화 특징을 분석하여 적용하기 위한 것으로 분산 분석과 그 단점을 극복하기 위해 Kalman 필터를 적용한 자기회귀 분석 모델이 연구되고 있다.

분산 분석을 적용한 자기회귀 모델은 트래픽이 특정 주기별로 유사한 패턴을 나타내는 비정류적인 특징을 분산 분석을 통해 월별, 요일별, 시간대별 요인을 제거하여 시간에 따라 평균의 변동이 없는 정류적 특성을 가지는 트래픽 데이터를 획득한다. 정류적, 비정류적 트래픽의 전형적인 패턴은 (그림 3)과 같다. 이후 이 데이터에 시계열 분석 모델인 자기회귀 모델을 적용하여 미래 값을 예측하고 이를 바탕으로 미래 실제 측정치가 한계치를 벗어날 확률을 계산함으로써 이상 유무를 판단한다. 그러나 분산 분석을 수행하기 위해서는 많은 양의 훈련 데이터를 필요로 한다[5].



(a) 정류적 트래픽 패턴

(b) 비정류적 트래픽 패턴

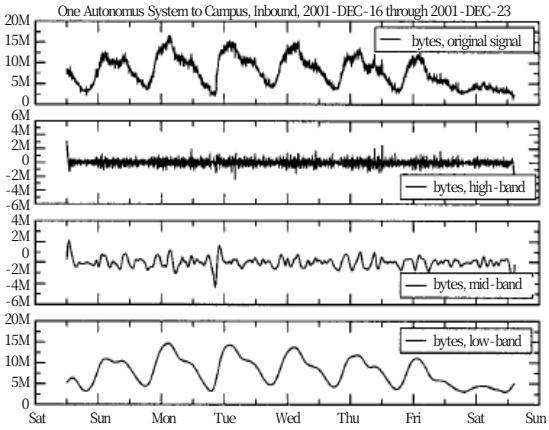
(그림 3) 트래픽 패턴

Kalman 필터를 적용한 자기회귀 모델은 Kalman 필터를 이용하여 트래픽의 비정류적 특성인 요일별, 시간대별 요인을 제거하고, 이렇게 구한 정류적인 데이터에 분산 분석에서 마찬가지로 자기회귀 모델을 적용하여 이상 트래픽 유무를 판정하였다. 이 모델의 경우 요일별, 시간대별 요인은 제거하였으나 월별 요인처럼 장기간에 걸쳐 나타나는 평균 변화를 고려하기 어렵다는 점이 단점이다[6].

• Wavelet 분석

Wavelet 분석은 트래픽 패턴을 전기적 신호로 간주하고 이를 각 주기별 트래픽 특성을 분리함으로써 각 주기별 비정상적인 트래픽을 탐지하는 데 좋은 수단을 제공한다[7]. (그림 4)에서처럼 원 트래픽의 시간대별 변화 특성을 단기, 중기, 장기별 트래픽 패턴으로 분리하여 분석함으로써 각 주기별 발생하는 이상 트래픽의 탐지에 적용할 수 있다.

단, 이 모델은 일정기간 수집된 트래픽에 대해서 사후 분석을 수행하므로 현 시점에서 발생하는 이상 트래픽 탐지에는 적용할 수 없다.



(그림 4) 트래픽의 단기/중기/장기 요소 분리

• 퍼지-자기회귀 분석

퍼지-자기회귀 분석은 비선형적이고 시간에 따라 변동하는 트래픽 패턴을 퍼지 클러스터링 기법을 이용하여 자기회귀 분석으로 근사화시키게 된다[8]. 이 모델은 트래픽 패턴을 자기회귀 모델로 세분화하기 위한 규칙을 바탕으로 입력 트래픽을 그 특성에 따라 해당 퍼지 셋으로의 대응기, 퍼지 셋으로부터 출력 데이터로의 대응기, 규칙을 바탕으로 출력 퍼지 셋을 결정하기 위한 추론 엔진 등으로 구성된다. 이 모델에서 퍼지 규칙이나 자기회귀 모형의 계수 증가는 계산의 복잡성을 증가시키지만 트래픽 패턴에 대한 정확한 모델을 제공하여 변동성이 심한 트래픽 패턴에 대해서도 미래 트래픽에 대한 정확한 예측을 수행함으로써 이상 트래픽 판정의 정확성을 높일 수 있다. 다만 그 계산의 복잡성으로 인해 (준) 실시간 처리가 어렵다는 점이 단점이다.

Ⅳ. 침해 요인에 대한 대응 방안

침해 요인에 대한 네트워크 차원의 대응은 크게 해당 침해 요소를 구성하는 트래픽의 블로킹(blocking), 필터링(filtering)에 의한 차단, rate limiting에 의한 완화, 라우팅 재조정에 의한 트래픽의 우회 등이 있을 수 있다. 이런 대응은 실제 트래픽에 대한 제어를 수행하기 때문에 현재의 네트워크 침해 요인에 대한 정확한 평가가 선행되어야 한다.

침해 요인 평가는 해당 침해 요인에 대한 심각도(severity)와 신뢰도(certainty)에 대한 평가로 볼 수 있다. 신뢰도는 침해 요인으로 판정된 것이 실제 공격에 의한 것인지 또는 그 영향이 네트워크 성능 저하를 실제로 유발할 수 있는지에 대한 것으로 이는 분석 모델의 동작의 정확성에 관한 내용이다.

심각도는 침해 유형에 대한 처리의 우선 순위에 관한 사항으로 판단된 침해 유형에 대해서 신뢰할 수 있다는 가정 하에 그 영향의 경중에 대한 등급 구분이 이루어지고 그에 따른 대응 정책이 결정되게 된다. <표 1>은 네트워크의 보안 상황에 대한 등급에 대한 구분을 보였다.

<표 2>에는 대표적인 대응 방안이라 할 수 있는 rate limiting과 필터링에 대한 특징을 보였다. 필터링은 해당 트래픽을 모두 차단하여 해당 서비스의 제공이 봉쇄되기 때문에 침해 요인 평가의 신뢰도가 높은 경우에 적용 가능하고 주로 사후 대응 방안으로 이용된다. Rate limiting은 일부 트래픽에 대해서 차단을 수행하므로 해당 서비스의 제공은 계속해서 이루어

<표 1> 네트워크 보안 상태 등급

보안 상태(등급)	설명
안전 상태 (green)	특이 징후 없으며 안전하다고 판단하는 상태
경계상태 (yellow)	간헐적 공격이 발생함으로 인해 일정 수준의 경계가 요구된다고 판단한 상태
준위험상태 (orange)	공격이 빈번히 발생하고 있으며 보다 엄격한 경계 및 일련의 대응이 요구되는 상태
위험상태 (red)	공격으로 인해 네트워크의 서비스가 더 이상 진행이 어려울 정도로 매우 위험하다고 판단한 상태이며 엄격한 대응이 요구되는 상태
감시불가상태 (dark)	보안 측면에서 현재 상황을 판단할 수 없는 상태

<표 2> Rate Limiting과 필터링의 기능 비교

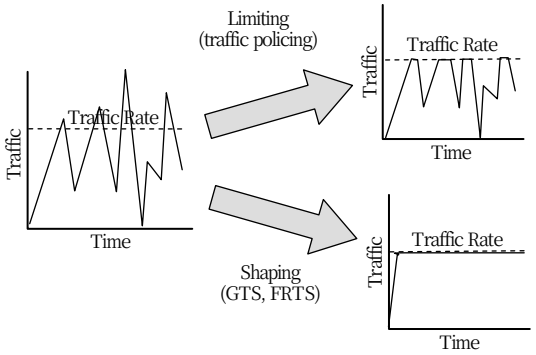
	Limiting	Filtering
사건대상	불특정한 사건에 광범위하게 묵시적으로 설정	개별/특정 사건에 대해 설정
적용대상	특정 호스트 보다는 서비스에 대해 보호	특정 호스트, 서비스에 대해 보호
생명주기	생명 주기가 길다	생명 주기가 짧다
적용기준	불명확한 원인에 대해 적용 가능	원인에 대한 명확한 결과에 기반 적용 가능

질 수 있다. 따라서 침해의 징후가 있을 경우에도 적용 가능하고, 이로 인해 중요 자원에 대한 사전 보호와 같은 적극적인 대응 방안으로 이용될 수 있다.

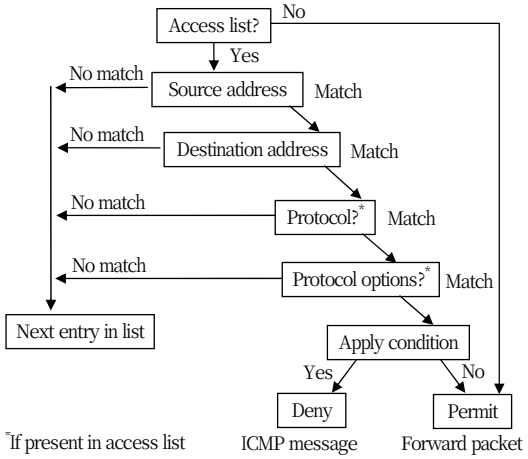
Rate limiting은 사전에 정의된 보안 정책에 따라 허용 트래픽 수준을 설정하고 그 이상을 초과하는 트래픽에 대해서는 네트워크 상에서 그 전달을 보장하지 않는 것이다. 주로 Leacky-bucket 알고리듬을 이용하여 구현되면 일정 수준을 초과하는 트래픽에 대해서 차단한다는 점에서 일정한 대역폭을 제공하는 traffic shaping과는 구분된다. (그림 5)에 rate limiting과 shaping의 차이에 대해 개념적 차이를 보였다.

트래픽 필터링은 ACL(Access Control List) 기반필터링과 uRPF(unicast Reverse Path Foward-ing) 기반 필터링으로 크게 구분된다.

ACL 기반 필터링은 보안 정책에 따라 특정 주소나 프로토콜을 구성하는 트래픽에 대해 차단 정책을 수행하는 것은 라우터 내부의 ACL을 제어함으로써 수행 가능하다. 공격 툴을 이용한 공격 트래픽에서



(그림 5) Traffic Rating 및 Traffic Shaping



(그림 6) ACL 기반 트래픽 필터링

주로 나타나는 예약된 주소, 할당되지 않은 주소, 유효하지 않은 주소 등을 가지는 트래픽에 대한 ACL을 작성할 수 있고 이를 통해 공격의 탐지 및 네트워크 상에서의 사전 차단이 가능하다. 그 전체적인 수행절차는 (그림 6)과 같다.

uRPF 기반 필터링은 패킷 반환 경로 상의 인터페이스와 패킷이 도착한 인터페이스가 동일한지를 검사하여 위조된 원천지 주소를 갖는 패킷을 필터링하게 된다. 만약 비대칭 경로가 존재하는 경우에는 부적절하기 때문에 백본 라우터보다는 에지 라우터에 적용하는 것이 바람직하다.

라우팅 재조정에 의한 대응 방법으로는 블랙홀 기법과 싱크 홀 기법이 있다. 블랙 홀 기법은 해당 침해 트래픽 패킷을 라우터의 bit bucket으로 전달함으로써 해당 트래픽을 차단하게 된다. 이 방법의

경우 목적지 주소 위주의 필터링에 적용되고 CPU와 ACL 처리 시간 절약으로 인해 성능 저하가 없고, 트래픽 폭주로 인해 네트워크 다운이나 서비스 중지가 발생할 경우에 적용 가능하다.

싱크 홀 기법은 honey net과 같은 네트워크 내 특정 지점으로 해당 트래픽을 우회시키는 것으로 BGP(Border Gateway Protocol) 라우터의 설치 지점에서 이 라우터에 대한 제어를 통해 이루어진다. 우회된 트래픽에 대한 추후 분석을 통하여 forensic을 수행할 수 있다.

V. 보안정책 연구 동향

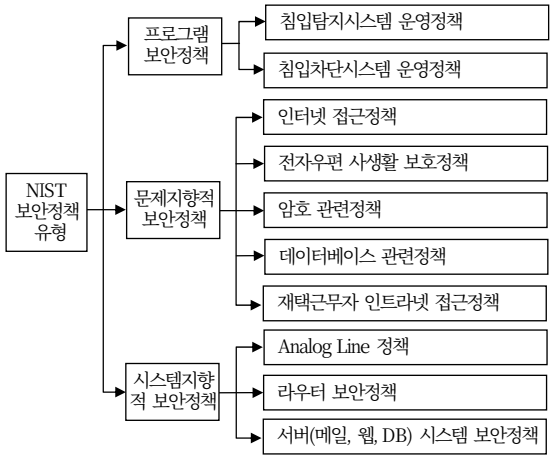
네트워크 보안에서 보안정책은 네트워크 및 이를 통하여 제공되는 응용 서비스에 대한 접근, 침해 요인의 탐지와 그에 대한 대응과 관련되어 해당 도메인에서 강제되어야 할 운용 규칙이다. 하지만 원래 보안정책의 주된 목적은 조직의 기술과 정보 자산을 보호하기 위한 필수적인 요구사항을 사용자와 운영자, 관리자에게 알려주는 것이고, 정책에 따라 컴퓨터 시스템과 네트워크를 취득하고 구성하고 감사하기 위한 기본 지침을 제공하는 것이다.

1. 보안정책의 분류

NIST(National Institute of Standards and Technology)는 보안 관련 프로그램을 효율적으로 관리 및 구성하기 위하여 설정하는 프로그램 정책, 각 기관별로 필요성이 제기되는 분야 혹은 사안에 대하여 적절한 행위를 규정하는 문제 지향적 보안정책, 개별적인 시스템 단위로 요구되는 보안항목을 정의하는 시스템 지향적 보안정책으로 분류하였고, 전체적인 분류방법은 (그림 7)과 같다[9].

Smith & Newton은 ISO 15408 1999 정보기술 보안평가를 위한 공통 기준(Common Criteria: CC)에 기반을 두어 CC 보호 프로파일 개발자를 위해 <표 3>과 같이 보안정책을 분류하였다[10].

기능 차원의 보안정책은 제품의 기능성과 대조되는 것으로써 기밀성, 무결성, 이용성, 신뢰성, 책임



(그림 7) NIST 보안정책 분류

<표 3> Smith & Newton의 보안정책 분류

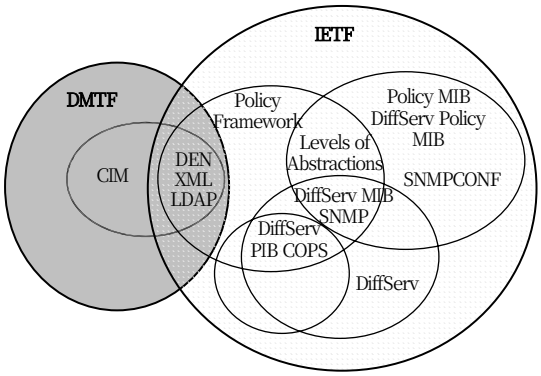
유형	요소
기능 보안정책	보안 서비스 제공 분야
보증 보안정책	제품 및 개발 분야
관리 보안정책	절차, 계획, 교육 분야

성, 부인봉쇄, 공통의 시스템 접근성 등을 포함하는 보안의 기능적 측면을 고려한다. 보증 차원의 보안정책은 제품 행위의 완성도, 개발환경의 안전성, 제품을 생산하는 데 있어 활용된 소프트웨어 개발 규율 등을 고려한다. 즉, 이러한 정책은 시스템 및 제품의 보증과 개발상의 보증을 포함한다. 관리 차원의 보안정책은 제품의 성공적인 활용 및 배치에 중심을 두고 있다. 훈련, 절차, 시스템 사용, 시스템 관리, 부수적인 사건에 대한 계획 등이 포함된다.

2. 보안정책 모델

보안정책 모델은 보안정책을 표현하고 관리 및 공유가 가능한 스키마와 그 스키마를 구성하는 클래스 계층구조로 제공되기 위한 것이다.

IETF(the Internet Engineering Task Force)와 DMTF(Distributed Management Task Force)에서는 (그림 8)과 같이 공동 표준화 영역으로 상호협조 하에서 네트워크 관리를 위한 정보모델링을 수행하고 있다.



(그림 8) IETF와 DMTF 표준화 그룹간의 관계

가. DMTF 표준화

DMTF는 통신망 장비와 서버의 하드웨어 자원, 시스템 자원, 응용서비스 자원 관리를 위해 계층별 기능과 시스템 차원의 관리객체 모델링에 관한 표준을 정립하고 있으며, 정책 기반의 네트워크 관리에 관련된 표준은 <표 4>와 같이 CIM(Common Information Model) Policy Ver.2.9를 제시하였다[11].

DMTF CIM은 데스크톱 개인용 컴퓨터를 관리하기 위한 표준을 제안한 DMI(Desktop Management Interface), 디렉토리 안에 네트워크 요소 및 서비스를 표시하기 위한 표준 정보모델을 제안한 DEN(Directory Enable Network), 인터넷상에서 웹을 기반으로 하는 네트워크 관리를 위한 정보모델과 이를 전달하는 메시지 전달 방식을 제안한 WBEM (Web Based Enterprise Management) 등을 기반으로 표준을 정립하고 있다. 특히 CIM은 XML (eXtensible Markup Language) 기반의 정보모델로 손쉽게 접속이 가능하도록 연구를 진행하고 있다.

또한 CIM_Policy29는 정책객체를 사용하는 사용자 또는 운영자의 접속에 대한 인증과 접속범위 설정을 위한 클래스, 정책 저장소로의 질의 조건 클래스, 외부 저장소에서 접속하는 방법을 설정하는 클래스가 정의되어 보다 충실한 보안정책 모델을 제공하고 있다.

<표 4> CIM Policy Specification V2.9

구성	관련 표준규격
Core	CIM_Core29
Application	CIM_Application29
	CIM_Application29_AppServer UML/PDF
	CIM_Database29
Device	CIM_Device29
Network	CIM_Event29
	CIM_Interop29
	CIM_IPSecPolicy29
	CIM_Metrics29
	CIM_Network29
	CIM_Physical29
	CIM_Policy29
	CIM_Support29
System	CIM_System29
User	CIM_User29

나. IETF 표준화

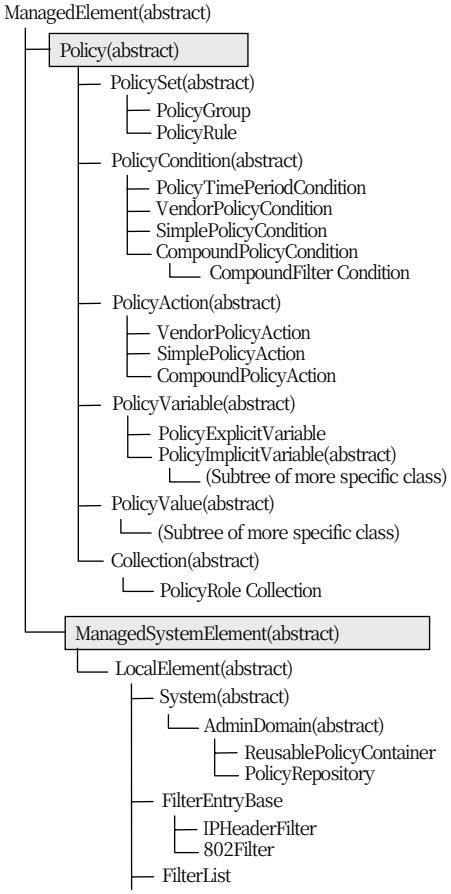
IETF에서는 <표 5>와 같이 시스템 제조자에 독립적이고 상호 운영이 가능한 정책모델인 PCIM (Policy Core Information Model)에 대해 RFC3060으로 기본 규격을 완성하였다[12]. PCIM은 DMTF의 CIM Ver.2.5를 기반으로 작성되었으며, 최근 PCIM에서 정의한 정책모델이 미흡하여, PCIM에서 부족한 부분을 추가한 PCIMe(PCIM extensions)로 재작성하여 RFC3460으로 규격을 제시하였다[13].

IETF PCIM은 DMTF의 CIM의 확장으로서 IETF의 정책 프레임워크 워킹 그룹과 DMTF에서 함께 개발하였고, 정책 정보를 표현하기 위한 객체 지향 정보 모델을 기술하고 있다. 이 모델은 정책의 제어와 정책 정보를 표현하는 구조 클래스(structural class)와 구조 클래스의 상호 연관성을 나타내는 연관 클래스(association class)를 정의하고 있다.

(그림 9)에 정책 핵심 정보 모델을 구성하고 있는 구조 클래스들의 상속 계층 구조를 보였고, PCIMe

<표 5> IETF 정책 핵심 모델 관련 규격

RFC	Specification Name	Date
3060	Policy Core Information Model	2001. 2.
3460	Policy Core Information Model (PCIM) extensions	2003. 1.



(그림 9) PCIMe 클래스 계층구조

주요 클래스의 역할은 <표 6>과 같다.

정책은 정책 규칙(PolicyRule)들의 집합을 사용하여 적용되고, 각각의 정책 규칙은 조건(Policy-Condition)의 집합과 동작(Policy-Action)의 집합으로 구성된다. 여러 정책 규칙은 정책 그룹(PolicyGroup)과 결합되고, 이러한 그룹은 정책들의 계층을 표현하기 위해 또 다른 그룹을 구성하게 된다.

이전에 살펴본 바와 같이, IETF에서의 정책모델은 정책모델의 핵심을 정의하였고, 특정 시스템에 적용할 때는 정책모델의 핵심을 기반으로 확장하여 사용하도록 하고 있다. 최근 IETF는 PCIMe 기반의 정책모델 핵심을 특정 시스템에 적용을 위해 <표 7>과 같이 세부정책모델로 확대하고 있다.

IETF IPSec CPIM은 트래픽을 주고 받는 주체, 각 주체들이 주고 받는 데이터 유형, 트래픽이 보호

<표 6> PCIMe 주요 클래스의 역할

클래스	주요 역할
PolicyGroup	연관된 *PolicyRule*들의 집합이나, 연관된 *PolicyGroup*들의 집합을 위한 컨테이너 클래스
PolicyRule	정책 규칙과 연관된 것으로 조건을 만족하면 동작을 취한다와 같은 의미를 표현하기 위한 클래스
Policy-Condition	정책 규칙에서 정책 조건을 나타내는 클래스
Policy-Action	정책 규칙에서 조건을 만족하면 수행되는 동작을 표현하는 클래스
PolicyTime-Period-Condition	미리 정해진 스케줄에 따라 정책규칙을 활성화 또는 비활성화시킬 수 있는 기능을 제공하는 클래스
PolicyRepository	정책과 관련된 정보를 위해 관리적인 측면에서 정의된 컨테이너 클래스

<표 7> IETF 세부정책 모델 관련 규격

RFC	Specification Name	Date
3585	IPSec Configuration Policy Information Model	2003. 8.
3644	Policy Quality of Service(QoS) Information Model	2003. 11.
3670	Information Model for Describing Network Device QoS Datapath Mechanisms	2004. 1.

되는 시점 등의 구성관리 측면에서 PCIMe 기반의 정책모델 표준규격을 제정하였다.

IETF QPIM은 PCIMe를 기반으로 정책기반의 QoS를 지원하게 하며, 비즈니스 차원의 정책을 정책 적용 디바이스로 정책을 제공하는 절차로 이루어진다. 네트워크 토폴로지와 운영방식, 서비스 제공 범위, 제어절차 및 방법론에 따라 QoS 요구 조건이 매우 다양하여 일관된 QoS 정책모델을 제시하기가 어렵다. 또한 디바이스 수준의 QoS 정책모델은 해당 디바이스에 따라 다르므로 RFC 3670과 같이 네트워크 토폴로지, QoS 범위, 제어방법을 설정하여 단계적으로 표준 규격을 제정하고 있다.

Ⅵ. 결 론

네트워크 차원에서 보안 침해 요인을 분석하고 이에 대한 대응 방안을 적용하고자 하는 노력은 최근

에서야 시작되었다.

이를 위해서는 기존의 보안 시스템으로부터 발생하는 다량의 보안 경보 이벤트에 대한 상호 연관성 분석과 네트워크 내 발생하는 트래픽에 대한 분석을 바탕으로 네트워크의 전체적인 보안 상황 분석이 필요하다. 또한 분석된 보안 상황을 바탕으로 네트워크 장비나 보안 장비를 제어하여 해당 침해 요인에 대한 대응을 수행함으로써 네트워크 서비스의 지속적이고 안정적인 제공이 담보되어야 한다. 또한 이런 일련의 보안 관리 과정에서 해당 도메인에 적용될 공통의 보안 정책을 모델링하고 관련 보안 장비에 강제하기 위해서는 관련 연구가 진행되어야 한다. 또한 이런 요소 기술들을 통합하여 목적하는 보안 기능을 수행하기 위한 각 보안 시스템에서 수행할 기능, 수행 기능 간의 상호 동작 형태, 통신 형태, 전체적인 기능 플로 및 구조를 정의할 전체 보안 프레임워크에 대한 정의도 필요하다.

이런 문제들을 해결하기 위해 기존에 행해졌던 연구들이 전체 네트워크 수준에서의 안정성 확보라는 목적을 염두에 두고 행해진 것이 아니라 개별적인 필요와 실제 적용할 영역이 각기 다른 상태로 이루어진 것이라 바로 적용하기는 어려우므로 추가적으로 상당히 많은 연구가 필요하리라 예상된다. 또한 네트워크 수준의 보안 기능이 제대로 수행되기 위해서는 기술적인 문제들의 해결뿐만 아니라 각 네트워크 도메인 운용 주체간의 보안 정보의 교환, 보안 관련 장비의 제어의 책임 소제 등과 같이 행정적인 문제도 해결되어야 한다.

하지만 경제활동이 네트워크에 더욱더 의존적이 됨에 따라 그 기반이 되는 네트워크 및 이를 통해 제공되는 서비스의 보안에 대한 방안이 강구되어야 할 것으로 보임에 따라 더욱더 많은 연구가 이루어질 것이다.

참 고 문 헌

[1] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer Worm," *IEEE Security and Privacy*, Vol.1, Issue 3, July 2003, pp.33-39.

[2] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "The Spread of the Sapphire/Slammer Worm," http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

[3] C.C. Zou, W. Gong, and D. Towsley, "Code Red Worm Propagation Modeling and Analysis," CCS'02, Nov. 2002, pp.138-147.

[4] C. Kolodgy and C. Christiansen, "ArcSight Vendor Profile: Seeing through the Clutter," IDC #26437, Feb. 2002.

[5] J.L. Hellerstein, F. Zhang, and P. Shahabuddin, "A Statistical Approach to Predictive Detection," Computer Networks, Vol.35, 2001, pp.77-95.

[6] F. Zhang and J.L. Hellerstein, "An Approach to Online Predictive Detection," *Proc. 8th International Symp. on Modeling, Analysis and Simulation of Computer and Telecommunication Systems,* Aug. 2000.

[7] P. Barford and J. Kline et al., "A Signal Analysis of Network Traffic Anomalies," *Proc. ACM IMW02*, 2002.

[8] B.S. Chen, S.C. Peng, and K.C. Wang, "Traffic Modeling, Prediction, and Congestion Control for High-Speed Networks: A Fuzzy AR Approach," *IEEE Trans. Fuzzy Systems*, Vol.8, No.5, Oct. 2000.

[9] NIST, "NIST Computer Security Special Publications," http://csrc.nist.gov/publications/index.html

[10] G. Smith and R. Newton, "IA Taxanomy of Organizational Security Policies," *Proc. 23rd National Information Systems Security Conference*, Oct. 2000.

[11] DMTF, "Policy Version 2.9 CIM Specification," 2004, http://www.dmtf.org.

[12] B. More and E. Ellesson et al., "Policy Core Information Model – Version 1 Specification," IETF RFC 3060, http://www.ietf.org/rfc

[13] B. More and E. Ellesson et al., "Policy Core Information Model Extensions," IETF RFC 3460, http://www.ietf.org/rfc