情 報 保 護 學 會 誌
第 15 卷 第 3 號, 2005. 6

조기경보를 위한 보안경보 연관성 분석 동향

김 진 오, 김 동 영, 나 중 찬, 장 종 수

요 약

특정 또는 불특정 네트워크를 공격 대상으로 하는 인터넷 웜, 분산서비스거부 공격 등의 출현과 가공할 파괴력으로 인해 네트워크에 대한 보안 요구가 점차 증가하고 있다. 침입탐지시스템 등의 네트워크 보안 솔루션은 네트워크 공격에 대한 감시 및 차단 등의 기능을 제공하며 기술적인 진화를 거듭하고 있지만, 근본적인 한계로써 국부 감시로 인한 불명확성과 오탐에 의한 보안경보[1]의 플러딩 등이 지적되고 있다. 특히 보안경보의 플러딩 현상은 네트워크 보안 상태를 정확하게 판단하는 것을 방해함으로써 조기경보체제의 구축을 어렵게 하는 요인이 되고 있다. 최근 이러한 부분을 극복하기 위해 보안경보 간의 상호 연관성 분석에 대한 연구가 활발해 지고 있다. 본 논문에서는 보안경보에 대한 연관성 분석 동향에 대해서 논의한다. 또한 보안경보의 집단화(aggregation)를 이용한 네트워크 공격 상황 분석 방안에 대해서도 논의한다. 보안경보의 집단화를 이용한 공격 상황 분석은 엄청나게 발생하는 보안경보로부터 조기경보를 위한 공격 정보의 판별과 광역 네트워크상에서 이상 현상의 탐지를 가능하게 한다. 이와 더불어 현재 ETRI에서 개발 중에 있는 네트워크 공격 상황 분석기인 NASA(Network Attack Situation Analyzer)에 대해서도 간략히 소개한다.

Ⅰ. 서 론

인터넷의 폭발적인 잠재력은 지속적으로 새로운 서비스를 창출해 내고 있으며, 현대 사회에서 경제뿐만이 아니라 사회적 인프라의 축으로 자리 매김하고 있다. 이러한 인터넷의 중요성은 인터넷이 마비될 경우의 사회적 손실과 혼란을 역으로 미루어 짐작할 수 있게 한다. 실제로 네트워크 공격은 지금 이 순간에도 일어나고 있으며, 공격의 파괴력은 갈수록 치명적으로 진화하고 있다. 우리는 이를 수년간에 걸쳐 실제로 행해 졌던 네트워크 마비 및 경제적 손실의 사례에서 쉽게 찾아 볼 수 있다.

사이버 공격은 특정 대상에 대해 해킹을 시도하는 단일 공격 형태에서, 특정 또는 불특정 네트워크를 대상으로 공격을 수행하는 다중 공격 형태로 변화하여 왔다. 이러한 사이버 공격 트렌드의 변화는 보안의 패러다임이 자신의 자산을 보호하기 위한 기관 또는 엔터프라이즈 중심의 보안으로부터 광역적인 협력 보안의 형태로 변모하고 있음을 암시한다. 예를 들어, SQL 슬래머 웜[1]에 의한 네트워크 마비는 특정 기관이나 엔터프라이즈에서 강력한 보안 솔루션을 채택한다 해도 그 영향에서 쉽게 벗어날 수 없음을 의미한다. 실제로 SQL 슬래머 웜에 의한 트래픽 증가로 인한 네트워크 마비 현상은 수많은 인터넷 온라인 업체에 엄청난 손실을 발생시켰다.[2-4] 그러므로 네트워크의 단일 지점에서의 개별적 감시만으로는 지속적이고 안정적인 서비스의 제공이나 네트워크 운용이 사실상 불가능하다.

네트워크 보안에 대한 위기의식은 침입탐지시스템, 침입차단시스템, 방화벽, 바이러스월 등의 다양한 보안 제품 개발을 촉진시켰다.[5] 이러한 보안 제품은 수상한 패킷을 감시하고, 제어함으로써 한층 네트워크 보안에 대한 안정감을 갖게 한다. 특히 침입탐지시스템은 수상한 행위를 감시하고, 그 결과를 관리자에게 알리는 기능을 제공함으로써 지난 수년간 가장 많이 설치된 네트워크 보안 구성요소 중 하나가 되었다. 그러나 침입탐지시스템의 가장 큰 단점 중 하나로 지적되어 온 것은 오탐에 의한 보안경보의 플러딩 현상을 들 수 있다. 침입탐지 시스템은 크게 오용탐지(misuse detection)와 비정상행위탐지(anomaly detection)

* ETRI 연구원 ({zyno21, kdy63281, njc, jsjang}@etri.re.kr)
1) 본 논문에서 보안경보는 침입탐지데이터(Intrusion Detection Message)와 동일한 의미로 사용한다.

의 두 유형으로 나뉠 수 있으며, 이 두 기법은 고유한 장점을 갖는다.[6] 그러나 침입탐지 기법에 관계없이 공격을 탐지하지 못하는 네거티브 오탐율[1]을 낮추기 위하여 약간이라도 의심스러운 행위를 보고하게 함으로써 결과적으로 높은 포지티브 오탐율[2]을 초래하게 되었다. 포지티브 오탐에 의한 보안경보의 플러딩은 관리자로 하여금 정확한 보안 상태의 파악을 어렵게 한다.

보안경보의 플러딩에 의해 발생할 수 있는 문제로는 심각한 이상 상태를 적절히 파악하지 못함으로써 적절한 조기 대응에 실패하는 상황을 들 수 있다. 이는 조기경보체제의 구축에 심각한 제약이 아닐 수 없다. 지난 수년간의 교훈에서 보듯이 이제 공격의 파괴력은 불과 수분 내에 엄청난 규모의 네트워크를 무력화 시킬 수 있을 정도이다. 또한 보안 전문가에 의한 분석은 엄청나게 발생하는 보안경보의 양에 의해 크게 위축될 수밖에 없으며, 이를 위해서는 결과적으로 많은 시간과 노력이 소요됨을 요구한다. 결국 폭발하는 보안경보로부터 보다 가치 있는 데이터를 추출하려는 노력이 요구되며, 이러한 노력은 보안경보에 대한 연관성 분석의 필요성에 부합한다.

보안경보에 대한 연관성 분석은 광역 네트워크에 대한 감시를 위해서도 필수불가결하다. 앞서 언급한 바와 같이 불특정 네트워크를 대상으로 하는 사이버 공격의 증가 및 공격의 엄청난 파괴력으로부터 네트워크를 보호하는 것은 단일 지점에서 수행되는 포인트 솔루션만으로는 사실상 어렵기 때문이다. 즉 전역 네트워크에 대한 보안 데이터의 수집과 이에 대한 분석이 없이는 국부 네트워크에 대한 보호는 가능할지라도 광역 네트워크에 대한 보호는 실제로 요원할 수밖에 없다.

본 논문에서는 네트워크상에서 발생하는 보안경보에 대한 연관성 분석 기법에 대해 논의한다. 2장에서는 현재 연구되고 있는 연관성 분석 기법에 대해 간략히 논의하고, 3장에서는 네트워크 공격 상황 분석 기법 및 현재 ETRI에서 수행 중에 있는 공격 상황 분석 기능 개발에 대해 간략히 소개한다. 끝으로 4장에서 결론을 맺는다.

II. 관련 연구

2.1 연구 동향

보안경보에 대한 연관성 분석의 초기 연구로써 그래프를 바탕으로 분산 공격을 판단하는 기능을 제공하는 GrIDS(Graph-based Intrusion Detection System)[7], 포지티브 오탐에 의해 발생하는 보안경보에 대한 필터링 기능을 제공하는 Complex Event Processor[8], 센서[3]로부터 보고되는 중복된 보안경보에 대한 판단 기능을 제공하는 EMERALD(Event Monitoring Enabling Responses to Anomalous Live Disturbances)[9] 등을 들 수 있다. 보안 측면에서의 연관성 분석은 이렇듯 다양한 방법으로 시도되어 왔지만, 이는 결국 두 가지 접근으로 나누어 생각할 수 있다. 하나는 단일 보안경보에 의해 판단 가능한 정보 이상의 유용한 정보를 찾기 위한 노력이며, 다른 하나는 개별적인 단일 보안경보의 분석 자체가 보안경보 플러딩으로 인해 불가능해질 수 있으므로 보안경보 간의 연관성을 찾아내 수많은 보안경보로부터 유용한 정보를 찾아내는 것이다.[10-12]

네트워크 공격의 경우 일련의 절차성을 보이며 수행되는 경우가 많다. 즉 특정한 공격을 위해서 선행 작업들이 요구되는 경우로써, 일련의 선행 작업들이 보편적인 절차를 갖는 경우를 의미한다[11]. 이러한 경우 앞서 언급한 바와 같이, 단일 보안경보에 의해서는 판단할 수 없는 행위를 보안경보 간의 연관성 분석에 의해 특정 절차를 수행하고 있음을 인지할 수 있다. 특히 이러한 분석에 의해 정형화된 공격 모델이 생성되게 되면, 선행 작업의 패턴에 기반하여 공격의 의지나 진위 여부를 판단할 수 있으며, 또한 포지티브 오탐의 감소와 더불어 향후 발생할 공격의 예측까지도 가능할 수 있다.

어떠한 경우, 단일 보안경보는 그 의미가 미비하더라도, 동일 특성을 갖는 보안경보가 다수 발생할 경우 이를 보다 심각하게 받아들일 수 있는 경우가 있다. 즉 동일한 속성을 갖는 보안경보가 반복적으로 발생하게 되면, 해당 속성의 공격을 좀 더 비중 있게 조망할 수 있음을 의미한다. 예를 들어 네트워크상에서 특정 공격이 빈번하게 발생하여 그 공격에 주의를 기울여야 한다는 것은, 다른 말로 표현하면 개별적으로는 서로 별개처럼 보이는 보안 경보들이지만 그 중에는 특정 공격이라는 동일한 속성을 갖는 보안경보가 네트워크상에서 만연함을 의미한다. 이를 연관 관계(correlation relationship)와 구분하여 집단 관계(aggregation relationship)로 표현하기도 한

1) 네거티브 오탐(율): false negative detection (rate)
2) 포지티브 오탐(율): false positive detection (rate)
3) 본 논문에서는 보안경보를 산출하는 네트워크 구성 요소를 **센서**라 표현한다.

다.[12] 이러한 집단 관계의 분석은 특히 초당 수십 건 이상 발생하는 보안경보 플러딩 하에서 상대적으로 비중 있는 공격 속성을 추출함으로써 네트워크상에서 발생하는 공격 상황 분석에 효과적으로 이용될 수 있다.

보안경보에 대한 연관성 분석 연구는 다음과 같은 세 가지 방향으로 요약될 수 있다.

2.1.1 중복성 분석 (Duplication Analysis)

중복성 분석은 단일 공격 이벤트에 의해 다수의 보안경보가 발생하는 경우, 이를 하나의 이벤트로 인식하는 기능을 수행한다. 이는 단일 이벤트에 의해 하나의 센서에서도 다수의 보안경보가 발생하는 경우와, 다수의 센서에 의해 다수의 보안경보가 발생하는 경우로 볼 수 있다. 이러한 경우에 대해 중복성 분석은 해당 보안경보가 단일 이벤트에 의해 생성되었음을 인지한다.

2.1.2 순차성 분석 (Consequence Analysis)

순차성 분석은 공격이 수행되는 절차를 이용하여, 보안경보 발생 시에 해당 보안경보에 대한 공격 의지를 판단하는 것이다. 특정 공격의 경우 논리적인 절차나 전략적 흐름이 존재할 수 있으며, 이러한 순차 체인은 일련의 보안경보에 대한 순서 그래프로 표현될 수 있다. 이러한 경우, 발생 보안경보의 패턴이 순차 체인과 같은 (또는 유사한) 패턴을 보인다면, 그 공격 의지가 높다고 판단 가능하며, 역으로 전후가 생략되고 발생한 단독 보안경보라면 이는 포지티브 오탐의 가능성이 높다고 생각할 수 있다. 이러한 순차성 분석은 공격 의지의 계량화된 평가와 더불어 진행 공격의 탐지 및 최종 공격 목표의 예측 등에 활용될 수 있다.

2.1.3 상황성 분석 (Situation Analysis)

상황성 분석은 동일 속성을 갖는 보안경보가 반복적이거나 지속적으로 발생하는 상황을 탐지해 내는 것이다. 즉 단일 보안경보의 경우는 그다지 심각하게 여겨지지 않을 수 있으나, 동일 속성을 갖는 보안경보가 반복적으로 발생하는 경우 때로는 이를 심각하게 여겨져야 하는 경우들이 발생한다. 예를 들어 분산서비스거부공격의 경우 특징적으로 특정 호스트로 향하는 보안경보가 다수 발생하게 된다. 이러한 경우 해당 호스트로 향하는 각각의 보안경보는 경미하게 취급되더라도, 특정 호스트에 대한 공격으로 특징화되는 상황이 발생한다면 이는 보다 심각하게 받아들여질 수 있다. 특히 상황성 분석은 보안경보 플러딩으로부터 가치 있는 공격 상황 정보를 판별하는 좋은 도구가 된다.

2.2 개발 동향

보안경보 연관성 분석 기능을 제공하는 솔루션을 유형별로 살펴보면 다음과 같다.

2.2.1 메모리 기반 대 DB 기반

보안경보 분석을 수행하는 방식에 따라 메모리 기반 방식(in-memory-based)과 DB 기반 방식(query-based) 으로 나눌 수 있다. 일반적으로 메모리 기반 방식은 보안경보에 대한 연관성 분석을 메모리상에서 수행하는 것을 의미하며, DB 방식의 경우는 보안경보를 DB에 적재하고, 보안경보 발생 시에 DB 질의를 이용하여 연관성 분석을 수행하는 것을 의미한다. 메모리상에서 직접 처리하는 메모리 기반 방식이 보다 높은 성능을 제공하나, DB 방식의 경우는 성능적인 면은 상대적으로 뒤처지나, 메모리 용량의 한계에 제약받지 않고 더욱 많은 데이터 셋을 이용한 분석을 수행할 수 있다는 장점이 있다. 따라서 메모리 기반 방식의 경우는 실시간 처리에, DB 기반 방식의 경우는 비실시간 처리에 각각 유용하게 이용된다.

2.2.2 규칙 기반 대 상태 기반

규칙 기반 방식(rule-based)의 경우는 일정한 패턴을 유지하면서, 보안경보의 발생 시에 그 패턴을 비교함으로써 보안경보 간의 상호 연관성을 찾아내는 방법이다. 이에 반해 상태 기반 방식 (state-based)은 발생 보안 경보들로부터 특징적인 현상이 발견되는지를 찾아내는 것이다. 그러므로 규칙 기반의 경우 알려진 공격 패턴에 대해서는 강력한 반면, 알려지지 않은 공격에 대해서는 패턴 적용이 용이하지 않은 단점이 있다. 반면에 상태 기반 방식의 경우는 알려지지 않은 공격에 대해서도 탐지가 가능하다는 잇점이 있다.

2.2.3 패키지 대 툴킷

보안경보 연관성 분석 솔루션이 어떤 형태로 제공되는가에 따라 패키지 형태와 툴킷 형태로 구분된다. 패키지 형태의 경우 독립 솔루션의 성격이 강하며, 툴킷 형태의 경우는 컴포넌트로써의 성격을 강하며, 일정 부분 환경에 따른 커스터마이징도 가능하다.

Ⅲ. 네트워크 공격 상황 분석

3.1 네트워크 공격 상황 분석

네트워크 공격 상황 분석은 기본적으로 상황성 분석에 근거하여 네트워크에서 특징적으로 발생하는 공격 상황을 판별해 내는 것이다. 이는 보안경보의 플러딩 현상으로부터 가치 있는 공격 정보를 산출할 수 있으며, 또한 단일 보안경보로는 판단할 수 없는 공격 상황에 대한 탐지를 가능하게 한다.

그림 1은 두 가지의 특징적 공격 상황을 보여주는데, (a)의 경우는 특정 호스트가 다른 특정 호스트를 공격하는 형태이며, (b)의 경우는 다수의 호스트가 특정 단일 호스트를 공격하는 형태이다. 그림 1-(a)의 경우에는 특정 호스트 주소로부터 특정 대상 주소로 진행되는 보안경보가 반복적으로 발생할 가능성이 크다. 이에 비해 그림 1-(b)의 경우에는 특정 단일 주소를 목적지로 갖는 보안경보가 다수 발생하게 된다. 이 두 경우 모두, 단일 보안경보로는 그 진위가 모호하더라도, 공격이 특징화됨으로써 그 진위와 의지가 보다 명확하게 된다.

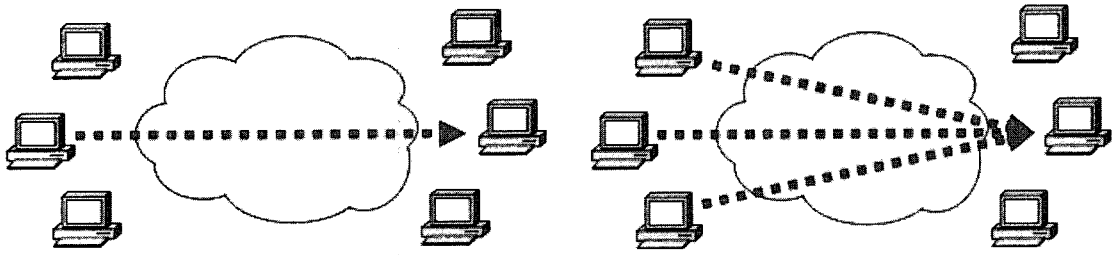
Debar와 Wespi[12]는 상황성 분석을 위해 보안경보의 세 가지 속성 - 소스 IP 주소, 목적지 IP 주소, 공격 클래스 - 을 이용하며, 이를 조합하여 총 7 가지의 특징적 상황으로 분류하였다. 즉 세 가지 속성이 모두 같은 경우를 Situation 1로 정의하였으며, 두 가지 속성이 같은 세 가지 경우에 대해 각각 Situation 2-1, 2-2, 2-3 으로 정의하였다. 끝으로 단일 속성만이 같은 세 가지 경우에 대해 각각 Situation 3-1, 3-2, 3-3 으로 정의하였다. 이를 위의 그림 1에 적용하면, 그림 1-(a)의 경우는 보안경보로부터 소스 IP 주소와 목적지 IP 주소가 같은 속성이 특징화 되므로 Situation 2로 표현될 수 있다 (즉 Situation 2-1, 2-2, 2-3 중의 하나). 그림 1-(b)의 경우는 특정 목적지 IP 주소의 속성이 특징화 되므로 Situation 3으로 표현될 것이다 (즉 Situation 3-1, 3-2, 3-3 중의 하나).

네트워크 공격 상황 분석의 구현 방법으로는 그래픽을 이용하는 시각화 방법과 동일 속성의 보안경보를 집단화하는 방법 등이 가능하다. 그래픽을 이용하는 시각화 방법의 경우는 시각적 요소를 이용하여 동일 속성을 갖는 보안경보 발생 시에 해당 특징이 그래프 상에서 선이나 면 등의 특징적 요소로 표현된다.[13] 즉, 특정한 패턴이 그래프 상에서 형상화되는 것이 바로 동일 속성을 갖는 보안경보에 의해 특징적으로 나타나게 되는 것이다. 반면에, 동일 속성의 보안경보를 집단화 하는 방법은 각 속성을 추출하고 이를 조합하여 동일 속성의 발생 횟수를 카운팅하고, 그 값이 임의의 제한 시간 이내에 특정 횟수 이상이 발생하게 되면 이를 공격 상황으로 판별해 낸다.

네트워크 공격 상황 분석은 다음의 두 가지 측면에서 유리하다. 하나는 포지티브 오탐에 의한 보안경보 플러딩으로 인해 적절한 분석과 대응이 어려워지는 현실을 감안할 때 동일 속성을 갖는 보안경보의 특징적 요소를 추출해 냄으로써 보다 가치 있는 정보를 제시할 수 있다는 것이다. 또 하나는 단일 보안경보에 의해서는 침해 여부에 대한 판단이 어려운 부분에 있어서 서비스거부공격이나 스캐닝 등과 같이 특징적인 패턴을 보이는 공격에 대해서는 높은 수준의 인지율을 제공하는 것을 들 수 있다.

3.2 NASA (Network Attack Situation Analyzer)

ETRI에서는 실시간의 효율적인 네트워크 공격 상황 분석을 위해 NASA를 개발하였다. NASA는 동일 속성의 보안경보를 집단화하며, 그 결과를 실시간으로 산출한다. 또한 기존의 7 가지 상황 유형 분류 대신 보안경보의 4 가지 속성을 조합하여 총 10 가지의 상황 유형으로 분류한다. NASA에서 이용하는 4가지 속성은 소스 IP 주소, 목적지 IP 주소, 공격 클래스



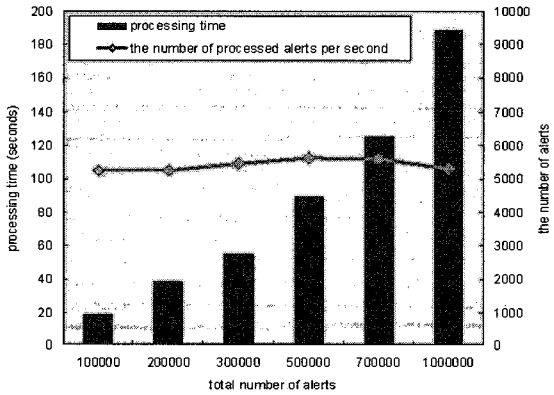
(a) one-to-one attack (b) many-to-one attack

[그림 1] 특징적 공격 상황

등 기존의 세 가지 요소에 서비스 유형 (IP 프로토콜 타입과 TCP포트 번호의 조합)의 요소가 추가적으로 이용되며, 분류되는 상황 유형은 표 1과 같다.

정확한 공격 상황 분석을 위한 중요한 요소 중의 하나는 어떤 데이터 셋을 이용하여 분석을 수행하느냐 하는 것이다. 우선, 현재까지 발생한 모든 보안경보를 대상으로 공격 상황 분석을 한다는 것은 큰 의미가 없다. 특히 공격 도구의 발달로 수 분 만에 네트워크에 대한 장악이 가능하기 때문에 과거 누적 데이터까지 이용하여 공격 상황 분석을 한다는 것은 왜곡된 결과를 동반할 개연성이 크다. 따라서 NASA에서는 분석에 이용되는 데이터 셋을 한정하고, 이를 모니터링 윈도우로 운용한다. 모니터링 윈도우는 분석에 이용되는 보안경보 데이터 셋을 유효 시간 내의 데이터로 한정한다. 또한 NASA는 다중 모니터링 윈도우에 대한 분석 기능을 제공한다. 이는 분석 대상 데이터 셋을 다양한 시간 범위로 설정함으로써 여러 시각에서 네트워크 공격 상황 트렌드를 분석할 수 있게 한다. 예를 들어 10분과 60분의 분석 윈도우를 유지한다면, 두 분석 윈도우의 결과는 상호 보완적인 결과를 산출할 수 있다.

또한 NASA에서는 보다 정교한 분석 결과를 얻기 위해 모니터링 윈도우를 시간 축에서 슬라이딩하여 분석에 사용되는 데이터 셋을 정교하게 유지하는 기법을 이용하며, 방대한 보안경보를 실시간으로 처리하기 위한 해쉬 기반의 고성능 처리 기능을 제공한다. 그림 2는 NASA의 성능 실험 결과를 보여 준다. 성능 실험은 4개의 2.4GHz Pentium-4 프로세서와 2G 메모리를 제공하는 리눅스 시스템에서 6개의 보안경보 데이터 셋을 대상으로 수행하였다. 실험 결과에서 보듯이 NASA는 데이터 셋의 크기에 영향을 받지 않고



〔그림 2〕 성능 실험 결과

〔표 1〕 NASA 공격 상황 유형

Situation Class	Source IP	Dest. IP	Attack Name	Service Type	설 명
1-1	Match	Match	Match		단일공격자로부터 특정호스트로의 특정 공격이 진행되는 상황, 예) TCP ACK flooding 등
1-2	Match	Match		Match	단일공격자로부터 특정호스트의 특정 서비스에 대한 공격이 진행되는 상황, 예) FTP command line overflow 등
2-1	Match	Match			단일공격자로부터 특정호스트로 공격이 진행되는 상황, 예) Smurf, Fraggle 등
2-2		Match	Match		특정호스트로 특정 공격이 진행되고 있는 상황, 예) 대부분의 분산서비스거부공격 등
2-3	Match		Match		단일공격자가 특정 공격을 진행하고 있는 상황, 예) 대부분의 스캐닝 공격 등
2-4	Match			Match	단일공격자가 특정 서비스에 대해 공격을 진행하는 상황, 예) UDP flooding과 같은 가미가제 공격 등
2-5		Match		Match	특정호스트의 특정 서비스에 대해 공격이 진행되고 있는 상황, 예) 분산서비스거부 공격 등
3-1	Match				단일공격자로부터 무작위 공격이 진행되는 상황, 예) 가미가제 공격 등
3-2		Match			특정호스트에 대해 공격이 진행되고 있는 상황, 예) DRDoS attack 등
3-3			Match		특정 공격이 네트워크에 만연하는 상황, 예) 대부분의 인터넷 웜 공격 등

초당 5,000개 이상의 보안경보를 처리한다.

Ⅳ. 결 론

네트워크 보안경보에 대한 연관성 분석은 방대하게 발생하는 보안경보로부터 가치 있는 공격 정보의 산출과 광역 네트워크에 대한 공격 상황 분석, 공격에 대한 의지 및 진위 여부의 판단과 더불어 진행 공격에 대한 예측 및 중복적으로 발생하는 보안경보에 대한 판별 등 다양한 목적을 이루기 위해 연구되고 있다. 이는 보안경보에 대해 보안 관리자가 일일이 분석하는 것이 사실상 불가능하며, 또한 단일 보안경보로는 판단할 수 없는 상황을 보안경보 간의 상호 연관성을 분석함으로써 판별해 낼 수 있기 때문이다. 특히 조기경보체제의 효과적인 구축을 위해서 이러한 보안경보에 대한 연관성 분석의 적용은 필수적이라 해도 과언이 아니다.

본 논문에서는 보안경보의 연관성 분석에 대한 연구 동향 및 개발 동향에 대해 살펴보고, 네트워크 공격 상황 분석 기법에 대해 논의하였다. 특히 본 논문에서는 공격 상황 분석을 위한 보안경보 연관성 분석에 대해 보다 세밀하게 살펴보았는데, 이는 발생 보안경보로부터 동일 속성을 갖는 보안경보를 추출하고 이들을 집단화(aggregation)함으로써 각각의 보안경보에 대한 분석으로는 찾아내기 어려운 공격 상황을 특징적으로 판별해 낼 수 있도록 한다. 이와 더불어, 본 논문에서는 현재 ETRI에서 개발 중에 있는 네트워크 공격 상황 분석기인 NASA에 대해서도 간략히 소개하였다. 향후 연관성 분석 기법은 조기경보체제 구축에 있어 일정부분을 자리매김할 것으로 예상된다.

참 고 문 헌

[1] CERT Advisory CA-2003-04, MS-SQL Server Worm, http://www.cert.org/advisories/CA-2003-04.html

[2] SQL Slammer Worm, Internet Traffic Report, http://www.internettrafficreport.com/ event/3.htm

[3] David Moore, Vern Paxson, Stefan Savage, http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html, CAIDA Technical Report; 2003.

[4] H. Kim, "Internet Traffic Control with reference to the Internet blackout of January 2003," NETSEC-KR (Network Security Workshop Korea), 2003.

[5] D. Schnackenberg, K. Djahandari, and D. Sterne, "Infrastructure for Intrusion Detection and Response," Proceedings of the DARPA Information Survivability Conference and Exposition, Hilton Head, SC, January 2000.

[6] Stefan Axelsson, Intrusion Detection Systems: A Survey and Taxonomy, Technical report 99-15, Chalmers University of Technology, Sweden, March 2000.

[7] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle, "GrIDS A Graph-based Intrusion Detection System for Large Networks," Proceedings of the 19thNational Information Systems Security Conference, October 1996.

[8] David C. Luckham and Brian Frasca, Complex Event Processing in Distributed Systems, Stanford University Technical Report CSL-TR-98-754, March 1998.

[9] P. A. Porras and P. G. Newmann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proceedings of the 20th NIS Security Conference, October 1997.

[10] A. Valdes and K. Skinner, "Probabilistic Alert Correlation", LNCS 2212, pp. 54-68, 2001.

[11] P. Ning, Y. Cui, and D. S. Reeves, "Analyzing Intensive Intrusion Alerts Via Correlation", LNCS 2516, pp. 74-94, 2002.

[12] H. Debar and A. Wespi, "Aggregation and Correlation of Intrusion-Detection Alerts", LNCS 2212, pp. 85-103, 2001.

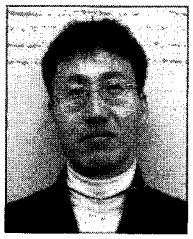
[13] H. Kim, J. Kim, S. Bahk, and I. Kang, "Fast Classification, Calibration, and

Visualization of Network Attacks on Backbone Links," International Conference on Information Networking(ICOIN), 2004.

〈著 者 紹 介〉

김 진 오 (Kim, Jinoh)
정회원

1991년 2월 : 인하대학교 전자계산공학과 졸업
1994년 2월 : 인하대학교 전자계산공학과 석사
1998년 2월~2001년 6월 : (주) 팍스콤 선임연구원
1991년 2월~현재 : ETRI, 현 선임연구원
〈관심분야〉 네트워크 보안, 네트워크 관리, 차세대 네트워크 구조 및 프로토콜

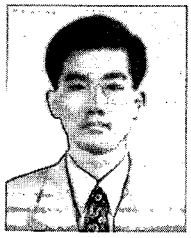


김 동 영 (Kim, Dongyoung)
정회원

1993년 2월 : 건국대학교 전자계산학과 졸업
1998년 2월 : 건국대학교 전자계산학과 석사
1998년 4월~2001년 8월: 윈베이스 소프트웨어
2001년 9월~현재 : ETRI 연구원
〈관심분야〉 정보보호, 프로그래밍 언어

나 중 찬 (Na, Jung Chan)
정회원

1986년 2월 : 충남대학교 계산통계학과 졸업
1989년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 컴퓨터과학과 박사
1989년 2월~현재 : ETRI, 현 능동보안기술연구팀 팀장
〈관심분야〉 비정상트래픽 분석, 네트워크 공격상황 분석, 네트워크 방어 시스템



장 종 수 (Jang, Jongsoo)
정회원

1984년 2월 : 경북대학교 전자공학과 졸업
1986년 2월 : 경북대학교 전자공학과 석사
2000년 2월: 충북대학교 컴퓨터공학과 박사
1989년 7월~현재 : ETRI, 현 네트워크보안그룹 그룹장
〈관심분야〉 네트워크 보안, 정책기반보안관리, 비정상트래픽 탐지, 유해정보 차단