특집

사이버 공격의 직관적 인지를 위한 사용자 인터페이스 기술동향 분석

차명석 · 심원태(한국정보보호진흥원)

Ⅰ. 서 론

최근 네트워크 기반 정보시스템의 비약적 발전은 산업 전반에 걸쳐 효율성 증대에 지대한 영향을 주었다. 이러한 흐름에 기초하여 정보시스템 인프라에 대한 산업 의존도는 급속하게 높아지고 있다. 정보기술 발전의 긍정적 영향의 이면에 정보자산에 대한 위협은 자동화되고 복잡한 기술을 응용하여 빠르게 진화하고 있으며, 국가 인터넷망의 마비를 초래한 지난 1.25 인터넷 침해사고에서 경험한 것과 같이 그 피해규모 또한 치명적으로 변모하였다. 최근의 보안 위협에 대해서 언급하자면, 알려지지 않은 소프트웨어의 보안 취약점과 좀비 네트워크를 거래하는 지하시장이 활성화가 진행되고 있으며, 좀비 네트워크의 주범인 IRC (Internet Relay Chat) Bot은 그 소스가 공개되고, 다양한 실행압축 기법을 이용하여 수많은 변종이 계속해서 발견되고 있는 상황이다. 이렇게 급속하게 변화하는 위협에 대응하여 관리 도메인의 보안 상태를 감지하는 다양한 기술이 정보시스템 인프라에 흡수되어 활용되고 있다. 그 예로써 현재 일반적인 조직의 보안인프라의 구성은 시그니처 기반 침입탐지시스템, 방화벽, 바이러스월 그리고 NMS (Network Management System)으로부터 보안이벤트와 네트워크 트래픽 데이터를 ESM (Enterprise Security Management) 솔루션을 통해서 수집하여 보안 관리자에게 전달되고, 이렇게 수집된 데이터를 이용하여 보안 관리자는 경험과 동향정보 등을 기반으로 침해사고를 판단하여 대응하도록 구성되어 있다. 하지만 급변하는 환경에 대응하기 위해서는 분석해야할 보안이벤트와 관련정보의 양이 기하급수적으로 증가하고 있는 추세이며, 이러한 보안 이벤트는 많은 탐지오류를 포함하고 있는 문제점을 가지고 있다. 이러한 이유로 수초안에 판단하여 대응해야하는 도래되는 치명적인 위협에 대해서 효과적인 대응방법을 찾아야 하는 현실적인 과제에 직면해있다. 본 고에서는 이러한 문제의 해법으로써 제시되고 있는 두 가지 기술에 대해서 소개하고자 한다.

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음.
[2005-s-606-02, 차세대 침해사고 예측 및 대응 기술]

첫째, 단편적 정보를 담고 있는 이기종 탐지센서로부터 발생하는 보안 이벤트간의 상관성 분석기술에 대한 동향과 전문가시스템을 기반으로 상관분석 시스템을 구현한 구체적인 사례를 설명한다. 둘째, 보안 이벤트를 사용자에게 효과적으로 가시화함으로써 관리 도메인의 보안상황 인지를 개선하는 시각화기술 동향과 그 사례를 소개하고자 한다.

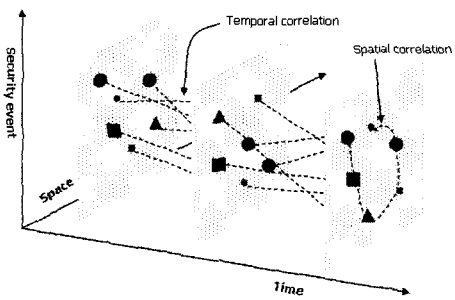
II. 상관분석을 이용한 보안상황 인지

보안 담당자는 매순간 수많은 이기종의 보안 이벤트를 중앙에 수집하여 상호 연관성 분석을 통해서 그 영향을 추론하여 관리 도메인의 보안 상황을 판단하고 침해사고에 즉시 대응해야 한다. 여기에서는 이러한 상관분석 기법에 대해서 설명하고자 한다. 먼저 상관분석은 단일 보안이벤트를 기반으로 하여 탐지하는 것 대신 복수의 보안이벤트를 연관된 규칙을 이용하여 공격을 탐지하는 방법을 말한다. 이러한 상관분석은 여러 보안이벤트에 분산되어 존재하는 공격의 증거를 종합하여 판단함으로써 보다 정밀한 공격탐지를 가능하게 한다[1]. 상관분석 과정에 대해서 간략하게 설명하자면, 이기종 보안 이벤트를 정규화된 입력정보로 변환하고, 많은 양의 입력을 유효시간 내에 처리할 수 있는 분석 프로세스를 통해서 측정 가능한 결과로써 도출하는 일련의 과정으로 설명할 수 있다. 이러한 상관분석을 통해서 획득 할 수 있는 세부적인 기능은 첫째, 중요하지 않은 보안 이벤트를 필터링하고 분석과정을 통해서 정제된 결과만을 사용자에게 전달함으로써 사용자가 관심을 가져야하는 보안이벤트의 양을 감소시킨다. 둘째, 기존의 시그니처(Signature)기반 침입탐지시스템과 임계값 설정을 통한 네트워크 트래픽 이상징후 탐지에서 발견되는 높은 오탐지율(False Positive)과 각 탐지센서에서 단편적 정보만으로 분석함으로써 탐지하지 못하는 미탐지율(False Negative)를 상관분석을 통해서 감소시킨다. 셋째, 보안 이벤트뿐만 아니라 네트워크 트래픽 정보와 같은 관리 도메인의 상황정보와 연관성을 분석함으로써 현재 발생한 위험의 심각도를 판정할 수 있다. 넷째, 수집된 모든 보안 이벤트와 상황정보를 분석하여 이전에 발생한 침해사고가 정보시스템에 어떤 영향이 주었는지 조사할 수 있는 포렌식(Forensics)기능을 포함한다[2].

1. 상관분석 기술 동향

여기에서는 보안 이벤트의 연관성에 대한 연구동향에 대해서 설명하고자 한다. 다양한 공격을 탐지하기 위한 보안이벤트간의 연관성은 크게 세 가지의 접근이 연구되고 있다.

첫 째, 공 간 기 반 상 관 성 (Spatial-based



〈그림 1〉 보안이벤트간의 연관성

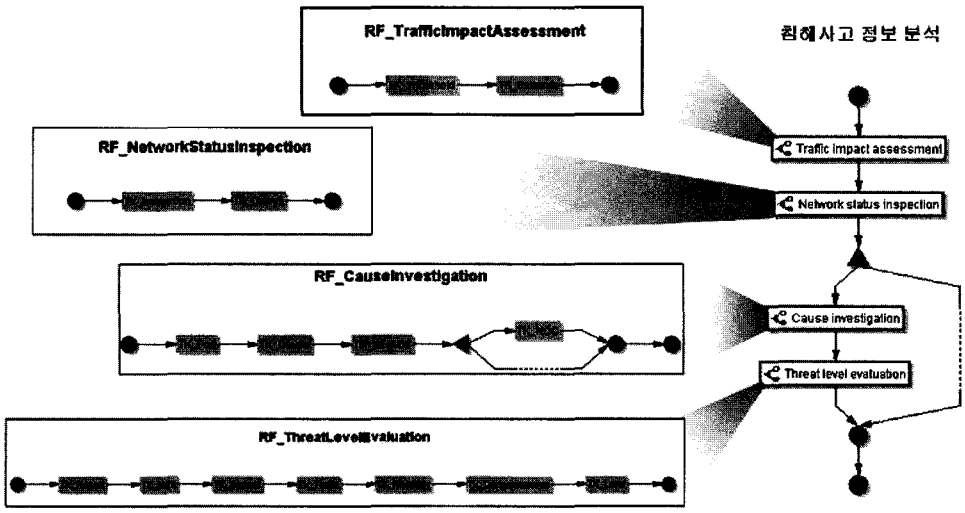
correlation)은 물리적으로 떨어져있는 여러 관측 장소 또는 서로 다른 탐지 센서에서 발생하는 보안 이벤트들 사이의 연관성을 찾는 것이다. 둘째, 시간기반 상관성(Temporal-based correlation)은 일반적으로 공격은 정보수집과 같은 사전준비에서 공격에 이르기까지 여러 단계를 거쳐 순차적으로 진행되므로 시간에 따른 보안 이벤트의 연관성을 찾는 것이다. 특히 이 접근은 보안 이벤트의 상태전이(State transition)로써 표현될 수 있다. 셋째는 위의 두개의 접근 방법을 결합한 공간과 시간기반 상관성(Spatial and Temporal-based correlation)이다[3]. 이러한 연관성을 찾는 방법으로 크게 두 가지의 방법이 연구되고 있다. 하나는 침해사고 분석 전문가의 도메인 지식을 지식베이스로 구축하여 사용하는 규칙기반의 전문가 시스템이며, 다른 하나는 누적된 보안 이벤트를 학습 데이터로 사용하여 특정 규칙을 찾아내는 데이터마이닝 기법이다[4]. 여기에서 상관분석 시스템을 구현하는데 있어서 분석속도와 탐지 정확도가 중요한 시스템의 성능척도가 된다. 전문가 시스템은 이기종 보안이벤트간의 연관 규칙을 미리 지식베이스로 구축하고, 입력되는 보안이벤트를 추론하여 결론에 이른다. 상관분석의 결과는 축적된 규칙의 효율성과 깊이에 종속적이므로 충분한 양의 전문가 지식을 이용한 지식베이스 구축이 요구되며, 그 분석속도가 신속한 것이 장점이다. 데이터 마이닝은 대표적인 기계학습 방법으로써 누적된 보안 이벤트에서 숨겨져 있는 데이터간의 관계와 패턴을 찾아내어 모델화하여 상관성을 추출하는 방법이다[5]. 많은 데이터 마이닝 기법 중에서 관계 규칙(Association rule), 클러스터링(Clustering), SVM(Support Vector Machines) 그리고 의사결정 트리(Decision tree)가 많이 사용된다. 하지만 데이터 마이닝 기법은 실용적인 시스템을 구축하는 데 있어서 분석 대상의 데이터 량이 증가함에 따라 분석의 복잡도가 급등하는 문제점을 해결해야 한다. 이런 문제점을 해결하고자 분산 데이터 마이닝이 그 해법으로써 최근 연구되고 있다[6]. 데이터마이닝 응용기술의 현실적 제약으로 인해서 규칙기반의 전문가시스템이 실시간 대응을 위한 해법으로 상용제품에 적용되고 있다.

2. 상관분석 전문가시스템

여기에서는 규칙 기반의 전문가시스템을 이용하여 공간기반상관성을 분석을 위한 시스템 구축을 예로써 설명하고자 한다. 해당 전문가시스템은 관리 대상 네트워크에 운영 중인 다양한 탐지센서의 보안이벤트와 네트워크 트래픽정보와 같은 상태정보를 입력으로 하여 침해사고 분석전문가의 지식을 기반으로 구축된 지식베이스를 이용하여 상관분석을 수행함으로써 침해사고를 탐지하고 그 원인, 위험도 그리고 대응책을 추론하는 것을 그 목적으로 한다. 이러한 상관분석 시스템을 구축하기 위해서 먼저 지식베이스를 구축해하며, 이를 위해서 침해사고 분석에 대해 지식 전문가(Knowledge Engineer)와 환경 및 업무분석을 선행해야 한다.

가. 침해사고 상관분석 지식 추출

<표 1> 에서는 4단계의 침해사고 분석과정을 보여주고 있으며, 침해사고 분석업무 정의



〈그림 2〉 침해사고 분석 프로세스

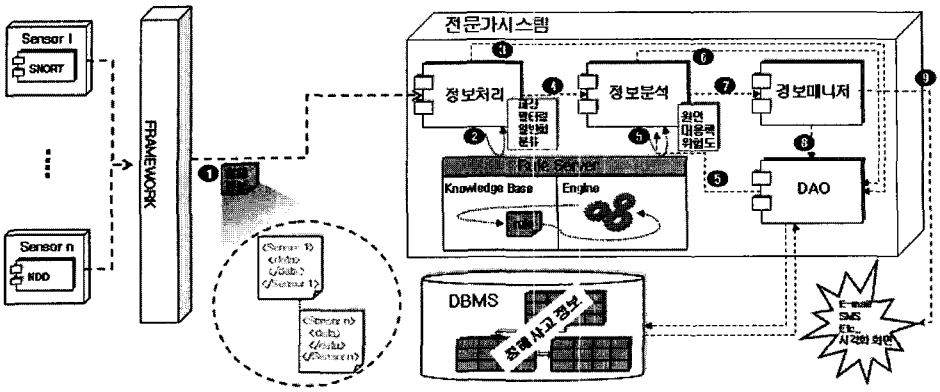
〈표 1〉 침해사고 분석 절차

단 계	내 용
네트워크 트래픽 영향분석	• 트래픽 통계분석 기반 네트워크 정상 모델 이용 • 정상적인 네트워크 트래픽 통계 모델을 기준으로 트래픽 영향도 산출
네트워크 서비스 상황분석	• 네트워크 링크의 가용대역폭, DNS등의 정보를 이용 • 네트워크 서비스 상태정보를 확인
원인분석	• 동일 시간대 탐지센서 이벤트 연관성 확인 • 관련 보안 취약점 데이터베이스와 웜 · 바이러스 연관성 확인
위험도 분석	• 트래픽 영향도, 복구 소요시간, 공격대상 중요도, 관련 사고 동향 등을 기준으로 위험도 산정

를 통해서 위의 그림과 같은 침해사고 분석 프로세스를 도출하였다. 다음 단계에서는 선행 정의된 프로세스를 기반으로 분기, 루프, 이벤트 대기, 서브 플로우 등으로 구체화하였다. 즉, 해당 프로세스를 구성하는 소단위 업무로 세분하고, 각 단위 업무별로 규칙그룹(Rule Set)으로 상세하여 판단트리(Decision tree)나 판단 테이블(Decision table)와 같은 적합한 유형으로 룰 표현 언어(Rule description language)를 이용하여 상세히 서술하였다. 단위 업무별 규칙그룹(Rule Set) 정의과정을 통해서 보안 이벤트, 트래픽 데이터 그리고 그 외 정보와 상호 연관 규칙을 정의할 수 있었다.

나. 상관분석 전문가시스템의 설계

상관분석 전문가 시스템을 구현을 위해 먼저 룰 표현 언어로 서술된 룰을 지식편집기(Knowledge editor)를 이용하여 지식베이스 구축을 선행한다. 여기에서 지식편집기는 지식베이스를 효율적으로 구축 및 관리하는 기능을 하며, 생성된 지식베이스의 문법오류(Syntax error), 유형 오류(Type error) 그리고



〈그림 3〉 상관분석 전문가시스템의 구성도

중복과 불일치에 대한 진단 또한 수행한다. 일반적으로 추론엔진에서 룰의 수가 증가함에 따라 룰 검사를 위한 소요시간이 급격히 증가하여 실시간 상관분석에 문제를 유발한다. 이러한 문제를 해결하기 위해서는 작업 메모리(Working memory)내의 심볼(Symbol), 각 룰의 조건, 해당 룰 등의 정보가 상호 유기적인 형태의 네트워크로 구성하여 룰의 탐사영역을 최적화하는 기법이 요구된다. 위의 그림 3은 상관분석 전문가 시스템의 구조를 보여주고 있으며, 중요 구성요소에 대해서 간략하게 설명하면, 각 탐지센서에서 입력되는 다양한 보안 이벤트는 정보처리 모듈에서 그 유형에 따라 분류되고, 정규화 규칙에 의해서 분류 및 일반화되며, 또한 이 과정에서 탐지센서별 필터링 룰을 기반으로 분석이 요구되지 않은 오류를 포함하는 보안이벤트는 분석단계로 진행되지 않도록 처리된다. 정보 분석모듈에서는 탐지된 공격에 대한 원인분석과 위험도 산정을 위하여 해당 시간에 발생한 이기종의 보안 이벤트와 네트워크 트래픽 정보를 지식베이스를 이용하여 상관 분석한다. 여기에서 탐지된 공격의 원인을 분석하기 위해서는 지식베이스이 이외의 최신의 취약점 정보와 웜·바이러스 정보를 필요로 한다.

III. 효과적 시각화를 통한 보안상황 인지

시각화(Visualization)는 다차원의 데이터를 2차원이나 3차원 기법을 이용하여 효과적으로 표현함으로써 사용자의 직관적 이해를 돕는 방법으로 정의할 수 있으며, 다양한 분야에서 시각화는 다차원 데이터를 직관적으로 이해하는 효과적인 방법으로 진화하였다. 또한 서론에서 언급한 바와 같이 네트워크 기반의 정보시스템 인프라의 정보보안을 위해서 복잡한 다차원 데이터의 정보를 효과적으로 인지해야 하는 문제가 존재한다. 특히 BcN과 같은 광대역 네트워크 인프라의 보급을 앞둔 시점에서 네트워크 트래픽 데이터를 연계한 보안

〈표 2〉 시각화의 특성

특 성	활 용
전달	• 사용자는 시각화를 통해서 이벤트 소스로부터 정보를 정확하고 효과적으로 전달 받는다.
분석	• 사용자와 시각화된 인터페이스를 통해서 효과적으로 분석을 수행한다.
탐색	• 사용자요구에 따른 데이터 탐색을 즉시 수행한다.
인지	• 수많은 복잡한 정보를 사용자에게 효과적으로 전달하여 상황인지를 돕는다.

분석은 매우 중요한 문제이다. 먼저 보안 분석 문제에서 시각화의 특성들이 어떤 측면에서 활용될 수 있는지 생각해보고자 한다.

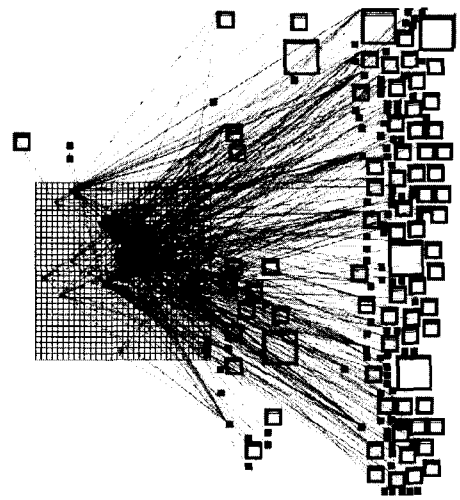
위의 표 2 에서 보이는 바와 같이 시각화는 보안 이벤트와 관련 데이터를 전달, 분석, 탐사, 인지의 특성을 통해서 사용자에게 관리 도메인의 보안상황 인지에 활용할 수 있다.

1. 시각화기술 동향

보안 이벤트관련 시각화 기술은 일반적으로 호스트의 상황을 보여주는 분야와 네트워크 상황을 보여주는 분야가 있으며, 많은 연구가 관리 도메인의 전반적인 보안 상황인지 인지에 관점이 맞춰져 네트워크 관련 시각화 연구가 활발히 이뤄지고 있으며, 여기에서는 이러한 네트워크 관점의 시각화에 대해서 소개하고자 한다. 네트워크 보안 관련 시각화 연구는 그 대상 데이터의 종류에 따라서 트래픽, 네트워크 침입탐지 이벤트, 혼합(Hybrid)으로 구분할 수 있다. 다음에서는 시각화 하고자 하는 데이터 유형에 따라서 구분하여 대표적인 연구내용과 실제 구현된 사용자 인터페이스를 설명한다.

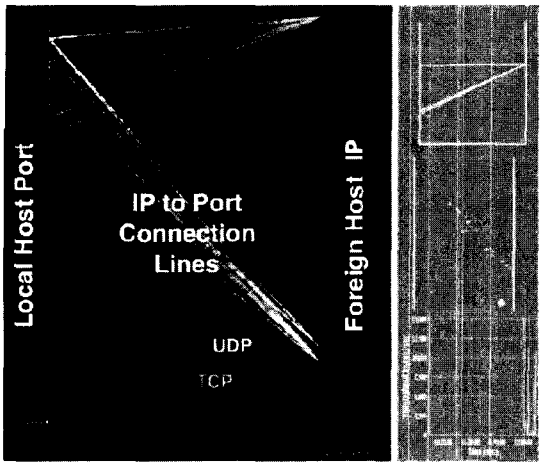
가. 네트워크 트래픽

일반적인 네트워크 모니터링은 트래픽 양과 패킷 개수를 프로토콜과 포트별 히스토그램(Histogram)을 관찰하여 수행된다. 네트워크 트래픽과 관련한 시각화는 트래픽 플로우 정보를 효과적으로 전달하는 연구가 활발히 이뤄지고 있으며, 서비스거부공격(DoS), 분산서비스공격(Distributed DoS), 정보수집(Finger printing, Host scan) 그리고 악성코드인 웜 전파 등의 모습은 출발 IP, 목적 IP, 목적 포트, 프로토콜 정보를 보여주는 플로우 분포를 분석함으로써 직관적으로 탐지 가능하다[7].



〈그림 4〉 VISUAL

그림 4는 VISUAL의 시각화 화면으로써 로컬 네트워크 IP와 외부 IP간의 플로우 분포를 사용자에게 전달하고자 한다. 그림 4에서 보이는 매트릭스 형태의 큰 사각형의 각 셀은 로컬 네트워크의 각 IP를 표현한 것이며, 크기가 서로 다른 사각형은 외부 IP를 표시한 것으로

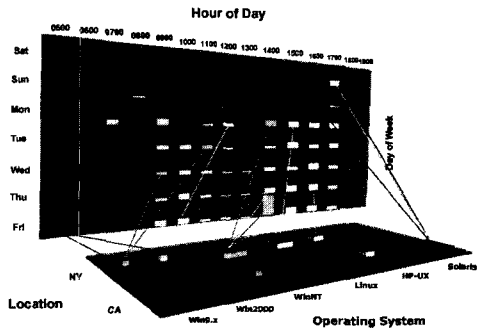


〈그림 5〉 Visual Signature view

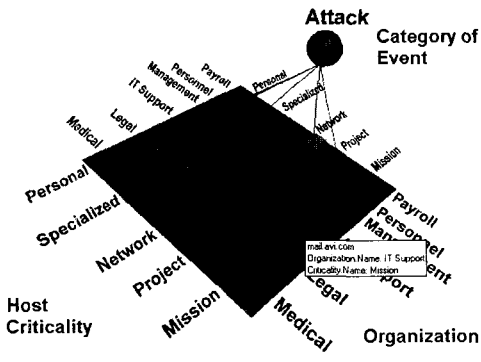
그 크기는 플로우의 개수를 보여준다[8]. 그림 5는 Visual Signature View로 외부 IP와 연결된 내부 포트에 대한 분포를 보여주며, 그림 5에서 왼쪽 y축은 내부 IP의 포트를 의미하며, 오른쪽 y축은 외부 IP를 의미한다. 그리고 연결선의 색상은 프로토콜의 유형을 표시한 것으로써 같은 색상의 연결선의 명도가 높은 것은 최근의 플로우이며, 오래될수록 점점 낮아져, 사용자가 최근 것과 오래된 것을 구분할 수 있도록 한다[9].

나. 네트워크 침입탐지 이벤트

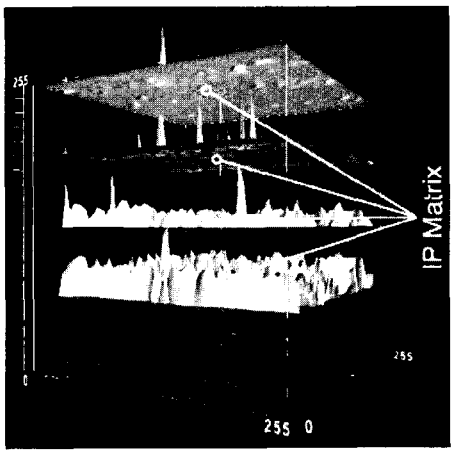
현재 네트워크 침입탐지시스템은 관리 도메인내의 각 중요 지점에 설치된 탐지 센서로부터 탐지된 공격관련 이벤트를 중앙의 데이터베이스에 수집하고, 이렇게 취합된 보안이벤트를 2차원의 차트나 리스트 형태로 단순한 정보만을 관리자에게 전달하고 있다. 하지만 보안 관리자는 공격을 이벤트를 확인하는 경우, 관리 도메인내의 공격 현황을 종합하여 그 심각성을 판단하고 대응책에 대한 결론을 도출해야 한다. 이러한 보안 관리자의 이해를 돕기 위해서는 물리적 위치에 따른 공격분포, 중요 서비스관련 관련성, 정보시스템 유형별 공격분포 등의 종합적인 정보를 제공해야 하는 문제가 존재하며, 이러한 요구에 대해서 최근 3차원 인터페이스를 이용하여 종합적인 정보를 전달하는 연구가 활발하게 진행되고 있다. 아래의 그림 6은 SecureScope의 Frequency-Wall view이며, 공격탐지 이벤트의 통계정보를 표시하는 것으로써 일주일 동안 장소와 운영체제별로 공격 탐지이벤트가 일별로 분포 현황을 보여준다.



〈그림 6〉 Frequency-Wall view



〈그림 7〉 3D Attack view

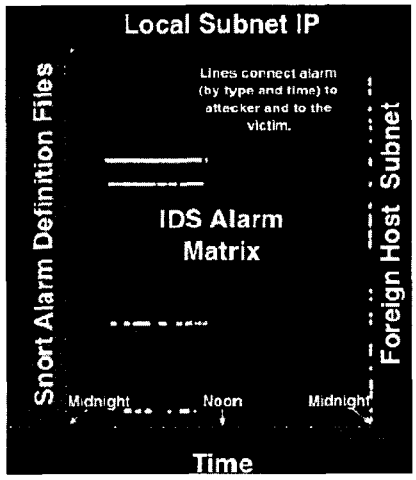


〈그림 8〉 IP Matrix 3D view

그림 7은 SecureScope의 공격탐지 이벤트를 탐지위치에 따라서 3차원으로 보여주며, 매트릭스 형태의 사각형은 부서와 업무에 따른 셀(Cell)로 구성되어 있다. 셀위의 여러 색상의 사각박스는 시스템이며, 그 색상은 각 운영체제를 의미한다. 그림 8은 IP Matrix의 3차원 View이며, 4 계층으로 구성되어 있다. 먼저 IP Matrix는 네트워크의 IP공간을 표현한 것으로써 IPv4의 4개 octet중 로컬 네트워크의 경우 3번째와 4번째가 가로축과 세로축의 값이 된다. 상위 3계층의 X축은 공격탐지 이벤트의 개수, 공격 전파정도, 운영체제를 의미하며 가장 아래 계층은 공격탐지 이벤트 개수를 투영하여 보여주는 것으로써 IP Matrix내에서 공격의 분포를 2차원의 정보로 확인할 수 있다[10].

다. 결합형

여기에서는 네트워크 트래픽 정보와 침입탐지 이벤트 데이터를 결합하여, 보다 종합적인 정보를 표현하고자 시도하는 시각화 연구를 소개하고자 한다. 아래의 그림은 Visual Firewall 연구에서 공개 네트워크 침입탐지시스템인 Snort의 공격탐지 이벤트와 네트워크 플로우의 관계를 보여주고 한다. 그림 9에서 왼쪽의 y축은 Snort의 탐지 시그니처, 중앙의 y축은 내부 IP, 오른쪽의 y축은 외부 IP를 보여준다. 내부 IP와 탐지 시그니처의 연결선의 색상은 공격의 횟수에 따라서 표현되며, 선은 최근의 공격과 플로우는 짙게, 오래된 공격과 플로우는 옅게 표현된다[9].



〈그림 9〉 IDS alarm view in a quad-axis

이상으로 다양한 보안관련 시각화 기법의 대표적인 사례를 살펴보았으며, 참고로 이상에서 소개한 방법 이외에 다차원의 데이터를 추상화하여 단순하게 전달하고자 하는 연구가 있으나, 본 고에서는 제외하고자 한다.

Ⅳ. 결 론

새롭게 부상하는 USN(Ubiquitous Sensor Network)와 BcN(Broadband convergence Network)과 같은 통합 네트워크 인프라의 구축을 진행하는 시점에서 지능화되어 가는 네트워크 기반의 위협은 해결해야 할 큰 과제임이 명확하다. 이러한 관점에서 신속한 위협에 판단 및 대응에 대한 필수요소인 관리 도메인의 보안상황인지에 대한 연구현황과 사례를 살펴보았다. 이와 같은 연구가 최근에 시작되고 있으며, 몇몇의 실효적 성과가 도출되고 있으나, 아직 다음과 같은 과제가 남아있다. 첫째, 보안상황 인지분야는 초기 연구단계로 이론적 지침을 수립하는 것이 시급하다. 둘째, 연구 결과를 검증하기 위한 충분한 기반 연구 성과에 대한 데이터베이스 구축이 필요하다. 셋째 실제 환경에 적용할 수 있는 수준의 연구 진행이 요구된다.

참고문헌

[1] H. Debar and A. Wespi, "Aggregation and correlation of intrusion-detection alerts", Proc. of the 4th Intl. Symposium on Recent Advances in Intrusion Detection(RAID'2001), Oct, 2001.

[2] C. Abad, J. Taylor, C. Sengul and W. Yurcik, "Log Correlation for Intrusion Detection: A Proof of Concept", 19th Annual Computer Security Applications Conference, Dec. 2003.

[3] Guofei Jiang and George Cybenko, "Temporal and Spatial Distributed Event Correlation for Network Security", Proc. of the 2004 American Control Conf., June 30-July 2, 2004.

[4] W. Lee and S. Stolfo, "Data mining approaches for intrusion detection", Proc. of the 7th USENIX security Symposium(SECURITY'98), Jan, 1998.

[5] Herbert A. Edelstein, "Introduction to Data Mining and Knowledge Discovery" , Two Crows Corporation, 1999.

[6] C. Aflori, F. Leon, "Efficient Distributed Data Mining using Intelligent Agents", Proc. of the 8th International Symposium on Automatic Control and Computer Science, Oct. 2004.

[7] A. Stephano and D. Groth, "USEable Security: Interface Design Strategies for Improving Security", 13th ACM Conterence on Computer and Communications Security Workshops (CCS'06 Workshops), Nov. 2006.

[8] R. Ball, G. Fink and C. North, "Home-centric Visualization of Network Traffic for Security Adminstration", ACM Conf. on Computer and Commun. Security's Workshop on Visualization and Data Mining for Computer Security(VizSEC), Oct. 2004.

[9] P. Lee, J. Trost, N. Gibbs, R. Beyah and A. Copeland, "Visual Firewall: Real-time Network Security Monitor", Proc. of the IEEE Workshop on Visualization for Computer Security (VizSEC'05), Oct. 2005.

[10] S. Noel, M. Jacobs, P. Kalapa and S. Jajodia, "Visualizing Cyber Attacks Using IP Matrix", Proc. of the IEEE Workshop on Visualization for Computer Security (VizSEC'05), Oct. 2005.

저자소개

차 명 석

1998년 2월 조선대학교 조선공학과 학사
2000년 2월 조선대학교 조선공학과 석사
2000년 8월-2002년 5월 (주)해커스랩 보안기술연구소 연구원
2002년 6월-2003년 7월 (주)하우리 컴퓨터백신기술팀 연구원
2004년 12월-2006년 12월 Carnegie Mellon University, PA, USA Visiting Researcher
2003년 8월-현재 한국정보보호진흥원 인터넷침해사고대응지원센터 선임연구원

주관심 분야 : Artifact analysis, Vulnerability analysis, Cyber Forensics, P3P, Network anomaly, Malicious code analysis

심 원 태

1986년 2월 서울대학교 계산통계학과 학사 졸업
1988년 2월 한국과학기술원 전산학과 석사 졸업
1987년 3월-2000년 9월 (주)데이콤 천리안개발2팀장
2000년 10월-2003년 3월 (주)인젠 연구소장
2003년 4월-2007년 5월 현재, 한국정보보호진흥원 분석대응팀장

주관심 분야 : S/W 취약점 및 웜바이러스 분석, 능동적 침해사고 대응기술