情 報 保 護 學 會 誌
第 16 卷 第 2 號, 2006. 4

보안 이벤트 시각화를 이용한 보안 상황 인지 기술

장 범 환*, 나 중 찬*, 장 종 수*

요 약

네트워크 보안 상황인지 기술이란 현재 네트워크에서 보안과 관련하여 무슨 일이 발생하고 있는 지를 관리자에게 인지시켜 주는 기술이다. 이는 침입탐지시스템이나 방화벽에서 수행하는 잠재적인 공격자의 패킷을 필터링하거나 보고하는 것과는 달리 현재 네트워크에서 발생하고 있는 상황(침입 또는 공격 등)을 알려주는 것에 초점을 맞춘다. 네트워크 보안 상황인지 기술에는 데이터 선정 및 수집, 특성 인자 추출, 연관성 분석, 데이터마이닝, 패턴분석, 이벤트 시각화 등과 같이 매우 다양한 세부 기술들이 있지만, 본 고에서는 이벤트 종류에 따른 시각화 기술들의 현황과 ETRI에서 개발한 *VisualScope*에 대해 살펴보고자 한다.

Ⅰ. 서 론

최근 국내외적으로 다양한 보안 이벤트 시각화를 통한 상황인지(Situational Awareness) 기술이 보안 관리에 있어서 화두가 되고 있다. 상황인지 기술이란 개개의 객체(이벤트, 사건)의 진위를 판단하고 규명하기 보다는 그것들의 연관성과 전체적인 패턴(동향)들을 통해 어떤 일이 발생하고 있고, 무엇을 해야 하는지를 알고자 함에서 출발한다. 사실 상황인지 기술은 인문·사회과학에 있어서 과거부터 연구되어온 학문 분야로써 보안 관리에 국한되거나 보안 분야의 새로운 기술은 아니다. 상황인지란, "당신 주변에서 진행되고 있는 또는 발생하고 있는 것을 아는 것, 그리고 당신이 알고 있는 범주 내에서 중요한 것이 무엇인가를 아는 것"이라고 정의할 수 있으며, 상황인지 단계는 식별(Perception), 이해(Comprehension), 예측(Projection)으로 구성된다[5][9].

식별은 다수의 센서(침입탐지시스템, 방화벽 등)들에서 발생하는 이벤트를 수신/저장하는 단계로써 발생한 이벤트의 시간과 종류, 그리고 센서에 대한 지식이 있어야 한다. 각 개별 센서들을 통해 전체 상황을 인지하기에는 아직 이르고, 이해를 준비하는 단계이다. 이해는 목표를 달성하기 위해 이벤트들을 통합 및 혼합, 재배치, 연관성분석 등을 수행하여 전체 상황을 표현한다. 예를 들면, 공격 개시 시간 및 공격자/피해자 시스템, 그리고 관리도메인의 피해 정도를 직관적으로 이해할 수 있는 형태로 표현하는 단계이다. 예측은 현재의 공격 상황 및 피해 정도를 토대로 대응 행동을 결정하도록 돕는 단계이다. 즉, 현재 진행되고 있는 의심스런 일련의 행동들을 토대로 공격자들을 파악하고, 그 공격이 계속 진행될 경우 피해 규모를 추론 및 완화시키거나 막는 방안을 관리자가 결정하도록 돕는다[5].

직관적인 네트워크 보안 상황인지를 위한 보안 이벤트 시각화 기술에는 크게 네트워크의 패킷 또는 트래픽 정보를 표현하여 이상 상황을 판단하는 것과 침입탐지시스템(IDS: Intrusion Detection System)이나 방화벽(FW: FireWall) 등과 같은 보안 장비들에서 발생하는 보안 경보를 표현 및 분석하는 기술이 있다. 이는 대상 이벤트 종류에 따른 분류인데 전자는 알려지지 않은 공격 패턴을 검출할 수 있는 장점이 있지만 방대한 이벤트를 처리해야 단점이 있다. 반면, 후자의 경우는 일목요연하게 여러 보안상황을 표현할 수 있는 반면 알려지지 않은 공격을 검출하는 데에는 한계가 있다.

Ⅱ. 보안 이벤트 시각화 기술 현황

보안 이벤트 시각화 기술에 있어서 보안이벤트 및

* 한국전자통신연구원 정보보호연구단 ({bchang, njc, jsjang}@etri.re.kr)

특성 인자의 선정은 매우 중요하게 고려되어야 할 사항이다. 보안 이벤트란, 네트워크의 보안상황과 관련 있는 모든 이벤트들의 집합으로 정의할 수 있으며, 크게 트래픽 정보와 보안 경보로 〔표 1〕과 같이 분류할 수 있다.

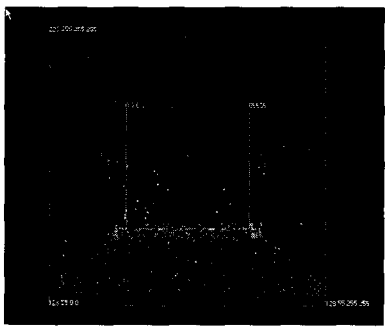
〔표 1〕 보안 이벤트 분류

이벤트 형태	이벤트 종류
트래픽 정보	- Packet, PCAP log, tcpdump log - Netflow, SNMP MIB
보안 경보	- IDS alert, Firewall log, ESM alert

2.1 트래픽 정보 시각화 기술

2.1.1 The Spinning Cube of Potential Doom

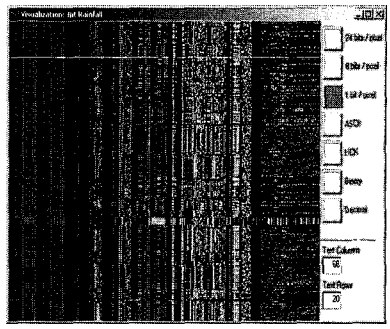
Spinning Cube는 NERSC(National Energy Research Scientific Computing Center)에서 개발한 보안 상황 인지 도구이다[10]. 3차원 공간을 구성하는 X축은 내부 IP 주소 범위, Z축은 전체 IP 주소 범위, Y축은 포트 범위를 의미한다. 주로 스캐닝 공격을 검출하는데 유용하며, 포트 스캐닝 공격일 경우 세로로 연속된 선이 나타나고 네트워크(호스트) 스캐닝 공격은 가로 형태의 선이 나타난다.



〔그림 1〕 Spinning Cube

2.1.2 RainFall, RainStorm

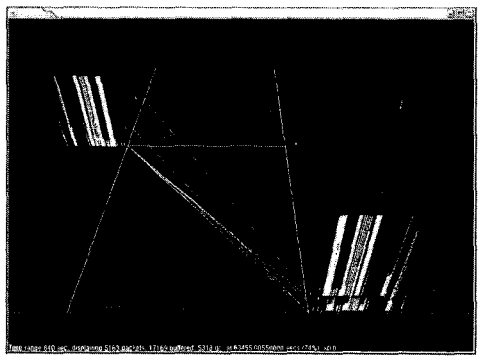
RainFall[1]은 2진수(bit)로 표현되는 트래픽의 헤더와 내용을 픽셀에 매치시켜 시각화함으로써 특정 근원지, 목적지, 프로토콜, 포트 등의 동일한 패턴을 찾는다. 반면에, RainStorm[1]은 IDS 이벤트를 이용하여 근원지/목적지 주소를 Y축, 시간을 X축으로 설정하고 네트워크의 상황을 표현한다. 이들은 현재 알려지지 않은 새로운 공격이나 패턴을 생성하는데 이용될 수 있다.



〔그림 2〕 RainFall

2.1.3 SecVis

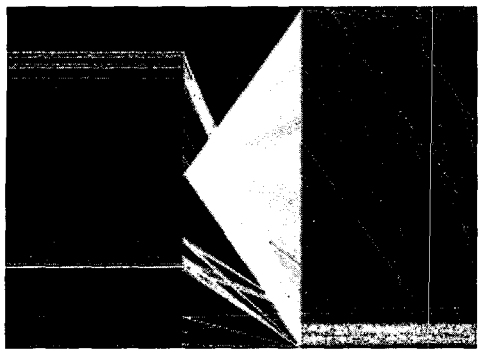
SecVis는 실시간 및 포렌직 분석에 이용 가능한 도구로써 전송되는 패킷을 캡쳐하여 그 정보를 3차원 상에 표현한다[8]. 좌측의 축은 근원지 IP 주소 범위, 우측의 축은 목적지 IP 주소 범위를 나타내고 있으며 근원지-목적지를 연결하여 세션을 표현하고 있다. 평면의 세로 막대는 패킷의 크기와 프로토콜(색깔)을 표현하고 있으며 오래된 데이터일수록 주소 축에서 멀리 떨어져 표현된다.



〔그림 3〕 SecVis

2.1.4 Visual Fingerprinting

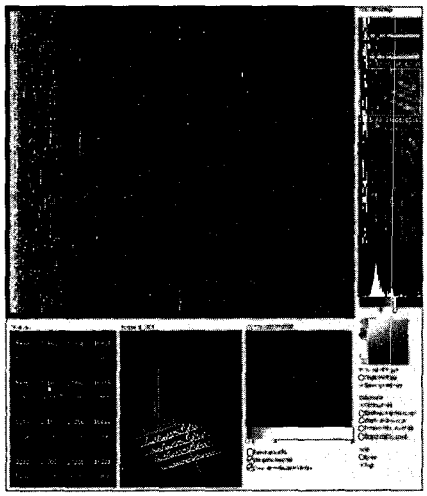
Fingerprinting은 네트워크 트래픽과 보안 상황을 감시하기 위한 도구로써 네트워크/호스트들의 트래픽 패턴을 실시간으로 표현하며 포렌직을 위한 상황 재연(playback) 기능을 포함하고 있다[3]. 일반적으로 네트워크 공격 도구들의 특징과 공격 이후에 나타나는 호스트들의 현상들을 표현한다. 이 도구는 웜(worm)과 분산서비스거부(DDoS: Distributed Denial of Service) 공격을 감시하기에 좋은 도구이다.



〔그림 4〕 Visual Fingerprinting

2.1.5 PortVis

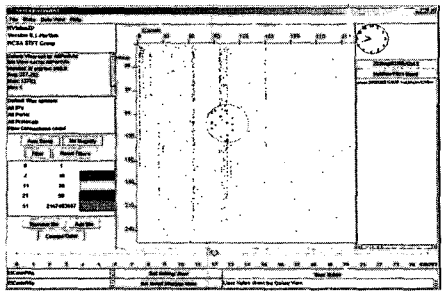
PortVis는 UC. Davis에서 개발한 도구로써 포트 기반의 네트워크 보안 상황 인지 도구이다[12]. 대규모 네트워크 환경에 적용할 수 있으며, 동일 정보를 여러 각도로 표현하여 관리자로 하여금 데이터간의 상호 연관성을 인지시킬 수 있다. 관리자는 표현 기간을 임의로 설정하여 네트워크를 감시할 수 있으며 비정상적인 현상들을 검출하기에 매우 좋은 도구이다. 기본적인 세분화(drill-down) 기능은 있지만, 해당 현상에 대한 상세 데이터를 표현하는 것은 제한적이다.



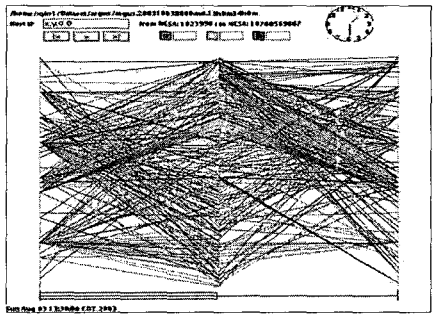
〔그림 5〕 PortVis

2.1.6 NVisionIP, VisFlowConnect

NCASSR(National Center for Advanced Secure Systems Research)의 SIFT(Security Incident Fusion Tool)는 보안 상황인지를 위한 대표적인 도구들로써 Cisco의 Netflow 데이터를 이용한다.



〔그림 6〕 NVisionIP



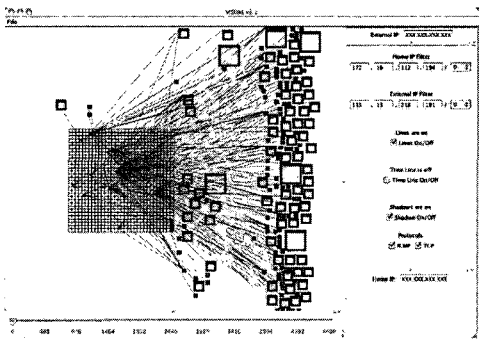
〔그림 7〕 VisFlowConnect

NVisionIP[9]는 클래스-B 주소 체계(a.b.c.d)의 네트워크(a,b) 부분을 가로축으로 삼고 호스트(c,d) 부분을 세로축으로 삼아 데이터들을 표현하고 있으며 포트들은 특정 색으로 할당하여 가독성을 높이고 있다. 전체 네트워크를 감시하는 Galaxy View를 포함하여 세부적인 특정 프로토콜 및 포트를 감시할 수 있는 Small Multiple Domain View, Machine View 등의 세분화 기능을 제공한다. VisFlowConnect[14]는 보안 상황 인지를 위해 세션(연결) 정보에 초점을 맞추고 있다. 패널 중앙에 내부 호스트들의 주소를, 좌·우측에는 외부 호스트의 주소를 표현한다. 표현된 연결선은 사전에 정의된 임계치를 초과하는 트래픽을 보여 주는 것인데, 연결선의 굵기로 트래픽 량을 표현하고 있으며 연결선의 색은 사전에 정의된 도메인을 의미한다.

2.1.7 VISUAL

VISUAL은 입력 데이터로 PCAP(Packet CAPture) 파일을 가공한 패킷 추적(trace) 정보를 이용한다. 일반적으로 공격자가 시도하는 포트 스캐닝, 핑(ping) 스캐닝 등을 쉽게 검출할 수 있으며 네트워크의 통신 패턴을 인지하기에 좋은 도구이다[2]. 1000개 보다 작은 호스트들로 구성되는 서브-네트워크의 포렌직(forensic) 분석에 이용되며 비정상적인 현상을 감시

하기에는 적절하지 않다. 세분화 기능을 위한 fan-in, fan-out 기능이 제공되며 시스템 로그나 IDS 로그는 사용하지는 않는다.

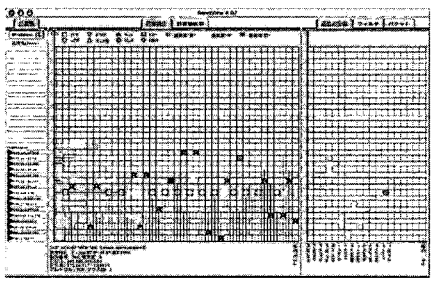


〔그림 8〕 VISUAL

2.2. 보안 경보 시각화 기술

2.2.1 SnortView

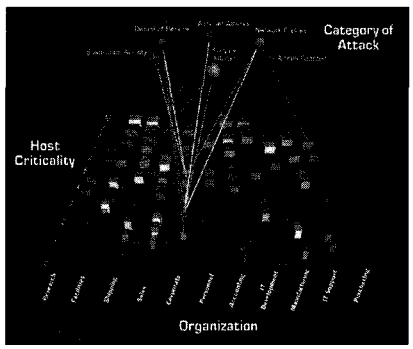
일본 전기통신대학에서 개발한 SnortView는 NIDS인 snort의 로그를 이용하여 이벤트들을 매트릭스 형태로 표현한다[7]. 근원지/목적지 IP 주소와 프로토콜 정보를 바탕으로 보안 경보 종류 및 우선순위에 따라 해당 이벤트(아이콘)와 중요도(색깔)를 표시한다. 이벤트의 개수는 막대그래프의 높이를 통해 알 수 있으며 해당 연결을 선택할 경우 근원지-목적지 간의 상세 정보를 화면 하단에 표시한다.



〔그림 9〕 SnortView

2.2.2 SecureScope

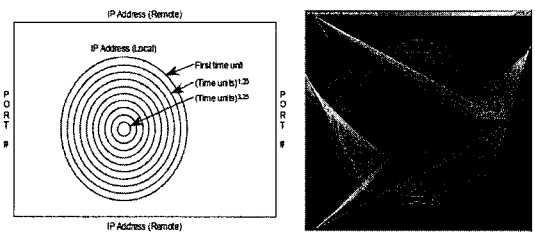
SecureScope는 Secure Decision 사에서 개발한 도구로써 IDS, Scanner, FW 등에서 발생하는 보안 경보와 그 보안 경보들의 연관성을 시각화한다[15]. 관리 네트워크(도메인) 내의 자원과 보안 경보를 함께 표현하여 현재의 보안 상황 정보를 보여주며 패턴 검색 및 동향에 대한 정보도 함께 제공한다. 특히, 이 도구는 보안 경보의 종류와 심각도 이외에 보안 경보들 간의 연관성을 결합하여 공격의 유형 및 이상 행동까지 보여 줄 수 있으며, 세부적인 호스트와 운영체제에 따른 보안 상황 정보도 제공한다.



〔그림 10〕 Secure Scope

2.2.3 IDS Challenges

Utah 주립 대학에서 개발한 이 도구의 공식 명칭은 없다. 침입 탐지를 주목적으로 하고 있으며, IDS 보안 경보 또는 PCAP(Packet CAPture) 로그를 이용한다[6]. 외부 사각형의 상/하 부분은 공격자의 주소를 좌/우 축은 포트번호를 대응시켜 나타내며, 공격자(src-ip, src-port)와 피해자(dst-ip, dst-port)를 모두 표시함으로써 공격 형태와 네트워크의 보안 상황을 〔그림 11〕과 같이 표시한다. 시간은 원형 축을 확장하여 공격의 진행 절차가 표시될 수 있도록 했다.

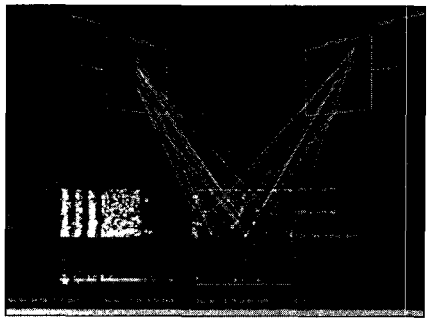


〔그림 11〕 IDS Challenges

2.2.4 Alert Plot

Iowa 대학교에서 개발한 Alert Plot는 NIDS 경보를 이용하여 보안상황을 표현하는데, 각각의 경보들은 5개의 우선순위에 따른 색깔로 대응되어 〔그림 12〕와 같이 표현된다[13]. 좌측 상단의 사각형은 클래스-B 주소 체계(a.b.c.d)에 의거한 네트워크(a,b) 주소를

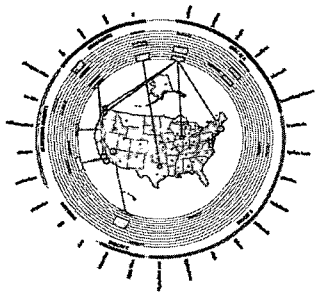
표시하고 우측 상단의 사각형은 관리 대상이 되는 네트워크의 호스트(c,d) 주소를 표현한다. 아래에 위치하고 있는 각각의 사각형에서 세로축은 포트번호를 의미하고 가로축은 시간의 경과를 나타낸다.



〔그림 12〕 Alert Plot

2.2.5 VizAlert, VisAware

Utah 대학에서 개발한 도구로써 IDS 보안 경보들의 특징(w3 premise: What, When, Where)을 기반으로 전체/개별 관리 도메인의 보안 상황을 시각화하는 기술이다. VizAlert[11]은 관리 도메인을 중앙에 두고 시간 주기를 의미하는 원들을 중심에서부터 외부로 표현하여 시간 경과에 따른 통계를 보여준다. 가장 외부에는 연관성 있는 보안 경보의 그룹들을 표현한다.



〔그림 13〕 VizAware

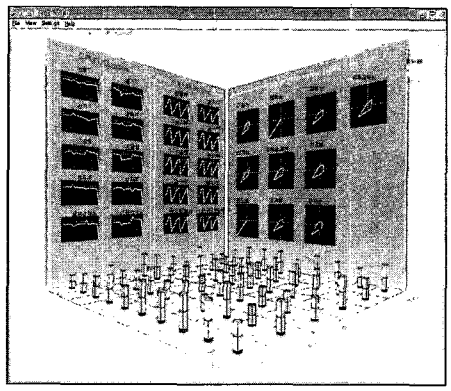
〔그림 13〕은 VizAlert을 개선한 VizAware[11]를 나타낸 것이다. 이 도구는 관리 도메인을 토폴로지 정보와 결부시켜 표현하며 보안 경보를 생성한 센서들의 정보를 가장 외부 원상에 표현하여 해당 보안 경보의 상세 정보를 제공한다. VizAlert과 VisAware는 네트워크 보안 상황 인지 이외에 범용적으로 911, 소방서, 경찰서 등과 같은 긴급구호 센터, 그리고 질병관리국의 BioWatch 등에 활용될 수 있다.

Ⅲ. VisualScope

현재 ETRI에서 개발한 네트워크 보안 상황 인지용 시각화 도구로써 VisualScope이 있다. 이 도구는 대량의 이벤트를 간단한 그래프(다각형)로 표현하여, 표현 처리 속도를 향상시키고 시스템에 의한 자동 대응을 가능하게 한다. VisualScope는 크게 네 가지 뷰(view)로 구성된다.

3.1 도메인 뷰(Domain View)

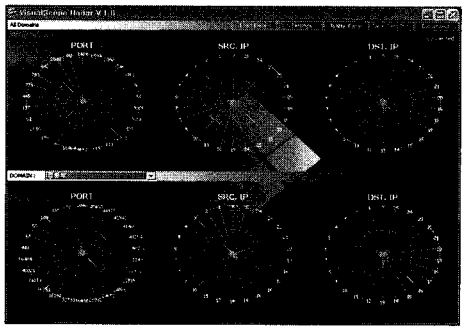
전체/세부 도메인별 보안 경보 및 트래픽 현황을 보여주는 도구이다. 보안 이벤트에는 IDS, FW, ESM, 트래픽 사이즈별 분포 이벤트가 있으며 도메인별 보안 정보에는 CPU 이용률, FW에 의한 폐기된 패킷 개수, 트래픽 현황 패턴 등이 있다. 트래픽 현황 패턴은 3종류의 사각형을 이용하여 현황을 표현한다. 도메인별 세부 트래픽 정보는 스펙트럼 뷰(Spectrum View)를 통해 확인할 수 있다.



〔그림 14〕 도메인 뷰

3.2 레이더 뷰(Radar View)

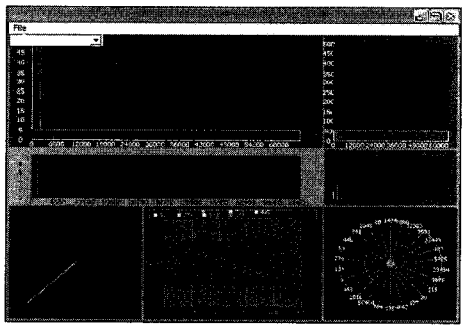
전체/세부 도메인별 트래픽 현황을 방사형 레이더를 이용하여 표현하는 도구이다. 각각의 레이더는 포트, 근원지 IP 주소, 목적지 IP 주소를 나타내며 상위 N개의 플로우 점유 비율을 점으로 표현 및 연결한다. 이상 트래픽 검출은 각 레이더에 임계치를 설정하여 점유비율이 해당 임계치를 벗어나는 지를 통해 알 수 있으며 임계치는 동적으로 설정 가능하다. 각 레이더에는 확대, 축소 기능이 있으며, 도메인별 세부 트래픽 정보는 도메인 뷰와 동일하게 스펙트럼 뷰를 통해 확인할 수 있다.



〔그림 15〕 레이더 뷰

3.3 스펙트럼 뷰(Spectrum View)

스펙트럼 뷰는 〔그림 16〕과 같이 세부 도메인별 트래픽 상황을 감시하기 위한 도구로써 동일한 트래픽 데이터를 다양한 각도로 표현한다.

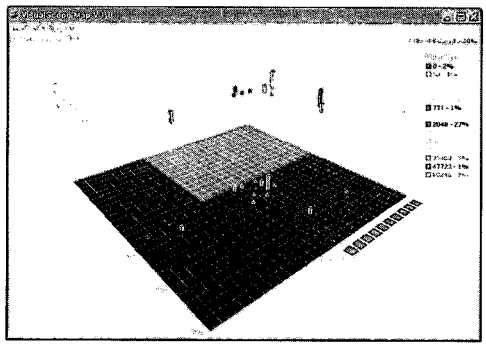


〔그림 16〕 스펙트럼 뷰

N구간(시간) 슬롯 동안의 포트별 트래픽 현황을 N×10 구간의 스펙트럼으로 표시하고 다시 10개의 통합 스펙트럼으로 표시한다. 따라서, 최대 N×10×10 구간의 포트별 트래픽 현황을 볼 수 있다. 빈도 수에 따른 가중치 부여는 허용된 픽셀(pixcel)에서 선의 폭과 색으로 구분한다. 선택된 슬롯은 하단의 플로우 사각형(Flow-Quad, Flow-Clock, N-Square), 세로 막대 그래프, 그리고 플로우 레이더에 표현된다.

3.4 그리드 뷰(Grid View)

전체/세부 도메인별 트래픽 현황을 근원지/목적지 IP 주소 범위로 이루어진 그리드 상에 표현하는 도구이다. 각 그리드는 근원지-목적지 간의 연결을 의미하며, 최다 점유를 차지하는 트래픽의 포트를 식별력을 갖는 색으로 표현한다. 이상 트래픽 현상의 검출은 가로 및 세로 열에 나타난 동일 색의 막대그래프(포트)의 개수와 그것의 합에 따라 결정되며 그 결과로 선택된 세로 열과 가로 열을 활성화시킨다. 예를들면, 인터넷 웜이 발생할 경우에는 특정 근원지에서 불특정 다수의 목적지로 동일 트래픽을 전송하기 때문에 특정 근원지 열이 활성화되고, DDoS와 같은 현상은 여러 근원지에서 특정 목적지로 트래픽을 전송하기 때문에 해당 목적지 열이 활성화되는 특징이 있다.



〔그림 17〕 그리드 뷰

IV. 결 론

본 논문은 네트워크 보안 상황 인지에 관한 소개와 보안 이벤트 시각화 기술 현황에 대해 설명하였다. 네트워크의 상황 정보를 시각화하는 목적은 트래픽의 이상 현상 및 패턴을 쉽게 찾을 수 있고, 방대한 데이터를 간략 명료하게 표현할 수 있으며, 또한 시스템에 의해 빠르게 표현 가능하고, 보안 관리자에게는 그 정보를 직관적으로(쉽고 빠르게) 전달할 수 있기 때문이다. 이것은 방대한 보안 이벤트 및 다양한 특성 요인으로 인하여 네트워크 보안 상황 인지가 어려운 지금의 보안 관리를 향상시킬 수 있다.

국내외적으로 보안 관리 현업에 종사하고 있는 관리자들의 최근 요구는 보안 상황 인지를 위한 시각화 기술이 주류를 이루고 있으며, 대부분의 도구들은 미국과 일본에 의해 개발되고 있다. 각각의 도구들마다 장단점은 있지만 공통적으로 이벤트 처리에 있어서 수행속도가 느리고, 표현된 패턴은 시스템이 자동으로 인지하기에는 매우 복잡하다는 것이다. 현재 ETRI에서 개발 중인 VisualScope 역시 보완해야 할 사항이 많이 있지만 앞서 지적한 도구들이 갖는 단점들을 찾아내고 그것들을 해결함으로써 기술 우위를 가질 수 있다고 생각한다.

참 고 문 헌

[1] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko, "IDS RainStorm: Visualizing IDS Alarms", *Proc. of VizSEC'05*, IEEE, pp. 1-7, Oct. 2005.

[2] R. Ball, G. Fink, and C. North, "Home-Centric Visualization of Network Traffic for Security Administration", *Proc. of VizSEC'04*, ACM Press, pp. 55-64, Oct. 2004.

[3] G. Conti and K. Abdullah, "Passive Visual Fingerprinting of Network Attack Tools", *Proc. of VizSEC'04*, ACM Press, pp. 45-54, October 2004.

[4] G. Conti, J. Grizzard, M. Ahamad and H. Owen, "Visual Exploration of Malicious Network Objects Using Semantic Zoom, Interactive Encoding and Dynamic Queries", *Proc. of VizSEC'05*, IEEE, pp. 83-90, Oct. 2005.

[5] A. D'Amico and M. Kocka, "Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned", *Proc. of VizSEC'05*, IEEE, pp. 107-112, Oct. 2005.

[6] R. Erbacher, K. Christensen and A. Sundberg, "Designing Visualization Capabilities for IDS Challenges", *Proc. of VizSEC'05*, IEEE, pp. 121-128, Oct. 2005.

[7] H. Koike and K. Ohno, "Snortview: Visualization system of snort logs", *Proc. of VizSEC'04*, ACM Press, pp. 143-147, Oct. 2004.

[8] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, "Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization", *Proc. of sixth IEEE Systems, Man and Cybernetics Information Assurance Workshop*, pp. 42-49., Jun. 2005.

[9] K. Lakkaraju, W. Yurcik, and A. Lee, "NVisionIP: netflow visualizations of system state for security situational awareness", P*roc. of VizSEC 2004*, ACM Press, pp. 65-72, Oct. 2004.

[10] Stephen Lau, "The Spinning Cube of Potential Doom", *Communications of the ACM, 47(6)*, ACM Press, pp. 25-26, Oct. 2004.

[11] Y. Livnat, J. Agutter, S. Moon, and S. Foresti, "Visual Correlation for Situational Awareness", *Proc. of IEEE 2005 Symposium on Information Visualization (InfoVis'05)*, Oct. 2005.

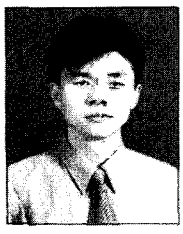
[12] J. McPherson, K. Ma, P. Krystosek, T. Bartoletti, and M. Christensen, "PortVis: A Tool for Port-Based Detection of Security Events", *Proc. of VizSEC'04*, ACM Press, pp. 73-81, Oct. 2004.

[13] A. Oline, and D. Reiners, "Exploring Three-Dimensional Visualization for Intrusion Detection", *Proc. of VizSEC'05*, IEEE, pp. 113-120, Oct. 2005.

[14] X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju, "VisFlowConnect: netflow visualizations of link relationships for security situational awareness", *Proc. of VizSEC'04*, ACM Press, pp. 26-34, Oct. 2004.

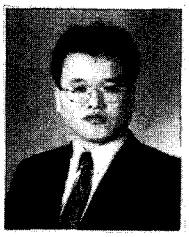
[15] SecureScope, Secure Decisions, http://www.SecureDecisions.com/

〈著 者 紹 介〉



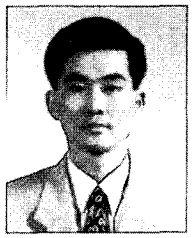
장 범 환 (Chang Beom-Hwan)
정회원

1997년 2월 : 성균관대학교 전자공학과 졸업
1999년 2월 : 성균관대학교 전기전자및컴퓨터공학과 졸업
2003년 2월 : 성균관대학교 전기전자및컴퓨터공학과 졸업
2003년~현재: ETRI 네트워크보안연구그룹 능동보안기술연구팀 선임연구원
관심분야 : 네트워크 보안, 보안 상황인지, 네트워크 트래픽 분석, 네트워크 공격상황 분석



나 중 찬 (Na Jung-Chan)
정회원

1986년 2월 : 충남대학교 계산통계학과 졸업
1989년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 컴퓨터과학과 박사
1989년~현재 : ETRI 네트워크보안연구그룹 능동보안기술연구팀 팀장
관심분야 : 네트워크 보안 관리, 보안 상황인지, 네트워크 트래픽 분석



장 종 수 (Jang Jong-Soo)
정회원

1984년 2월 : 경북대학교 전자공학과 공학사
1986년 2월 : 경북대학교 전자공학과 공학석사
2000년 2월 : 충북대학교 컴퓨터공학과 공학박사
1989년~현재 : ETRI 네트워크보안그룹 그룹장
관심분야 : 네트워크보안, 정책기반보안관리, 비정상트래픽탐지, 유해정보차단