Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1197

대규모 네트워크의 효과적 보안상황 인지를 위한 벌집 구조 시각화 시스템의 설계 및 구현*

박 재 범,[1†] 김 휘 강,[1] 김 은 진[2‡]
[1]고려대학교, [2]경기대학교

Design and implementation of the honeycomb structure visualization system for the effective security situational awareness of large-scale networks*

Jae-beom Park,[1†] Huy-kang Kim,[1] Eun-jin Kim[2‡]
1Korea University, 2Kyonggi University

요 약

컴퓨터 네트워크 규모의 지속적 확장과 함께 방화벽, IDS, IPS 등의 각종 보안 시스템들은 네트워크 보안과 관련해 더욱더 막대한 양의 정보를 생성하고 있어 보안 담당자가 그 속에 숨겨진 보안 위협의 징후를 탐지하는 일은 더욱 어려워지고 있다. 보안 담당자들의 '네트워크의 보안상황 인지'(Network Security Situational Awareness)는 여러 관점에서 발생하는 보안 이벤트들 사이의 관계에 기초하여 전체적인 컴퓨터 네트워크의 보안 상황을 효과적으로 판단하는 것으로 이의 과정은 크게 '식별', '이해', '예측'의 3단계로 나눠지며, '식별'과 '이해'는 그 뒤에 이어지는 '예측'과 적절한 대응의 전제 조건이 된다. 그러나 다량의 정보들 속에서 '식별'과 '이해' 과정은 더욱 어려워지고 있다. 본 논문은 다량의 정보들의 '식별'과 '이해' 단계에 효과적인 것으로 알려져 있는 시각화 기법을 적용하여 대규모 네트워크의 보안상황 인지를 돕기 위해 설계한 '허니컴' 시각화 시스템을 제안하고, VAST Challenge 2012의 데이터를 기반으로 실증적인 효과를 확인하였다.

ABSTRACT

Due to the increase in size of the computer network, the network security systems such as a firewall, IDS, IPS generate much more vast amount of information related to network security. So detecting signs of hidden security threats has become more difficult. Security personnels' 'Network Security Situational Awareness(NSSA)' is effectively determining the security situation of overall computer network on the basis of the relation between the security events that occur in the several views. The process of situational awareness is divided into three stages of the 'identification,' 'understanding' and 'prediction'. And 'identification' and 'understanding' are prerequisites for 'predicting' and the following appropriate responses. But 'identification' and 'understanding' in the vast amount of information became more difficult. In this paper, we propose Honeycomb security situational awareness visualization system that is designed to help NSSA in large-scale networks by using visualization techniques known effective to the 'identification' and 'understanding' stages. And we identified the empirical effects of this system on the basis of the 'VAST Challenge 2012' data.

Keywords: situational awareness, security visualization, honeycomb structure

접수일(2014년 10월 6일), 수정일(2014년 11월 14일), 게재확정일(2014년 11월 14일)

* 본 논문은 미래창조과학부 및 정보통신산업진흥원의 '지식정보보안인력양성 최고정보보안전문가과정' 사업의 연구결과로 수행되었음(과제번호 : NIPA-H2102-13-1002)

† 주저자, jaeburi@gmail.com

‡ 교신저자, ejkim777@kyonggi.ac.kr(Corresponding author)

I. 서 론

나날이 증대되고 있는 컴퓨터 네트워크 규모로 인해 국가기관, 기업 등의 보안 관리자들은 확장된 네트워크의 규모와 비례하는 수많은 PC, 보안장비 등의 시스템들이 쏟아내는 막대한 양의 보안 정보들을 분석해야하는 상황에 놓이게 되었다. 이러한 상황은 보안 관리자들로 하여금 그 속에 숨겨진 보안 위협에 대한 중요한 정보를 인지해 적절한 대응을 하는 것을 더욱 더 어렵게 하고 있다.

지난 2013년 국내에서는 '3.20 방송금융망 사이버테러', '6.25 정부기관 등 사이버테러'라는 범국가적 규모의 사이버테러 사건이 연이어 발생하였다. 이 사건들의 피해기관들은 대부분 언론, 금융, 정부기관 등과 같이 수많은 시스템들로 구성된 네트워크를 운용하는 곳들로, 대규모 네트워크의 보안상황 인지의 어려움을 드러내며 보안 실패의 결과를 단적으로 보여 주었다.

대규모 네트워크 보안 담당자들의 '네트워크의 보안상황 인지'(Network Security Situational Awareness)의 어려움은 상황인지 이론으로 설명될 수 있다. 상황인지 분야의 저명한 학자인 Mica Endsley는, 상황인지란 "주변에서 진행되고 있는 무언가를 알고, 알고 있는 범위 내에서 중요한 것이 어떤 것인지를 아는 것[1]"이라고 설명하고 있다. 즉, 상황인지란 모든 것을 아는 것이 아니라, 결정을 내리는 순간에 올바른 결정을 하기 위해 필요한 것들을 아는 것을 말한다.

상황인지의 과정은 크게 식별(Perception), 이해(Understanding), 예측(Predicting)의 3단계로 나눠진다. 이 중 ①'식별'은 주어진 환경 속에서 반드시 알아야 하는 요소를 감지하는 것이며, ②'이해'는 감지된 요소들을 종합하여 정해진 목표에 맞게 의미를 도출하는 것이다. 그리고 ③'예측'이란 '식별'과 '이해'를 토대로 다가올 미래에 기대되는 이벤트들을 미리 예상하는 것으로, 다음의 행동에 필요한 결정을 돕게 된다[2].

네트워크에 대한 보안 상황인지에 있어서도 '식별'과 '이해'는 네트워크 관리자 등이 '예측'을 통해 적시에 적절한 의사 결정과 대응을 하는데 있어서 중요한 전제조건이 된다. 하지만, 네트워크 규모와 함께 급격히 증가하고 있는 네트워크 보안 정보들로 인하여 이제 '식별'과 '이해'는 순수한 인간의 능력만으로는 감당할 수 없게 되었다.

시각화는 막대한 정보의 '식별'과 '이해'에 효과적인 방법으로 이를 네트워크 보안 분야에 적용한 시각화 연구가 최근 다양하게 이루어지고 있다. 네트워크 보안 시각화 기술은 네트워크상의 여러 시스템들이 생성하는 보안과 관련된 정보들을 이미지 등을 활용해 시각화하는 기술로 네트워크 관리자 등의 사용자에게 즉각적으로 인지되기 때문에 다량의 정보를 텍스트에 비하여 더욱 효과적으로 전달할 수 있다.

본 논문에서는 기존의 네트워크 보안 시각화 기법들이 네트워크 보안상황인지를 위한 '식별', '이해'의 측면에서 가지는 장단점들을 살펴보고, 대규모 네트워크의 보안상황인지에 있어서 더욱 효과적으로 '식별'과 '이해'를 도울 수 있는 시각화 시스템을 설계·구현하고자 한다.

2장에서는 보안상황인지의 '식별', '이해' 단계에 있어 기존 네트워크 보안상황인지 시각화 기법들을 살펴본다. 3장에서 이러한 기존 기법들의 분석을 토대로 새로운 형태의 보안상황 인지 시각화 시스템인 '허니컴' 시각화 시스템을 제안하고, 세부적인 디자인을 설명할 것이다. 4장에서는 모의 테스트를 통해 허니컴 시각화 시스템의 효과성을 실증적으로 확인하고, 마지막으로 5장에서는 결론과 함께 향후 과제를 제시하고자 한다.

II. 선행연구 검토

네트워크 보안상황인지를 위해 시각화에 이용되는 보안 이벤트 정보는 크게 ① NetFlow, Packet, PCAP log, tcpdump log 등의 트래픽 정보와 ② IDS alert, Firewall log, ESM alert와 같은 보안 경보의 두 가지로 나눌 수 있다[3].

이러한 분류에 따른 기존 시각화 도구들의 사례를 살펴보고, 각 도구들이 '식별'과 '이해' 측면에서의 장단점들을 직접 분석한 결과는 다음과 같다.

2.1 트래픽 정보 시각화 기술

2.1.1 NVisionIP

NVisionIP는 NCSA의 SIFT(Security Incident Fusion Tool) 프로젝트의 일부분으로 개발된 어플리케이션으로 Argus NetFlow 데이터를 이용해 class-B 대역의 IP 전체의 트래픽 흐름을 하나의 화면에 표현해준다[4].

NVisionIP를 분석해 보았을 때, 이의 장점은 각각의 트래픽의 유무를 점의 형태로 최소화하여 하나의

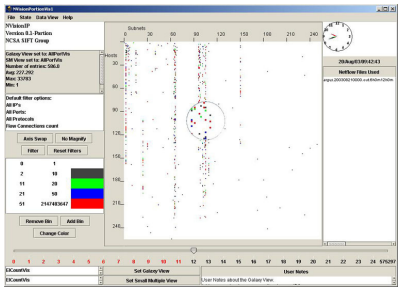

Fig. 1. NVisionIP

화면에서 전체 네트워크의 트래픽 흐름 파악이 가능하게 되어 '식별'을 효과적으로 할 수 있다는 것과 제공되는 단계적 시각화가 '이해'에 필요한 세부적인 정보를 제공하도록 구성되어 있다는 것이라 할 수 있다.

그러나 트래픽이 감지된 각각의 시스템들을 점을 형태로 표현함으로 인해, 각 시스템의 상태를 정확히 '식별', '이해'하는데 필요한 최소한의 정보를 함께 표현할 공간이 부족하다. 따라서 기본적인 '식별', '이해'를 위해서도 세부 정보를 확인하기 위한 시각화 단계에 반복적으로 진입해야만 하는 단점을 가진다.

2.1.2 VisFlowConnect

VisFlowConnect는 외부 domain들과 내부 시스템들 간의 네트워크 트래픽 흐름을 나타내기 위해 '평행축 표현'(parallel axes representation)을 사용하는 시각화 도구로서, 입력 데이터로 NetFlow 데이터를 사용하지만 다른 소스의 데이터도 사용 가능하다[5].

VisFlowConnect의 시각화 목적은 내부 호스트들과 외부 머신들 간의 관계를 방향과 트래픽 양을 포함하여 시각화해 보여주는 것이다. 2차원의 평면상에 표시된 평행한 축들은 각각 내부 또는 외부의 시스템들의 그룹을 나타내며, 축 상의 한 개의 점은 하나의 IP를 할당받은 시스템을 나타낸다. 그리고 각각의 축 위에 점으로 나타난 시스템들을 잇는 선은 해당 시스템들 간의 데이터 흐름을 표시한다.

VisFlowConnect는 축 상에 나타나는 시스템들의 범위를 제한하거나, 통신포트, 프로토콜, 패킷크기 등을 기준으로 필터링할 수 있는 기능을 제공하여, 도구의 사용자가 관찰이 필요한 특정한 트래픽 정보에 집중할 수 있도록 해준다. 또한 하나의 화면을 통해서 전체 네트워크의 트래픽 흐름을 관찰할 수 있게 해준다.

그러나 평행 축을 기반으로 화면에 표시되는 선들의 집합을 토대로 네트워크 전체의 상황을 식별하는 과정이

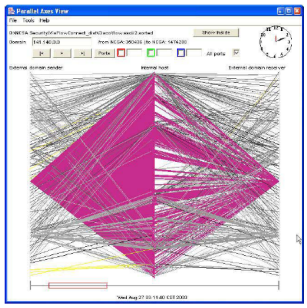

Fig. 2. VisFlowConnect

직관적이지 않으며, 특히 대규모 네트워크상에서 특정 시점에 트래픽이 다량 발생할 경우에는 너무 많은 선들이 화면을 가득 채우게 되어 '식별'이어려워진다.

2.1.3 FloVis

FloVis는 네트워크 데이터 흐름의 다양한 측면을 보여주기 위해 디자인된 시각화 도구의 모음이다. 각각의 이미지들은 다른 이미지들을 보완하며, 서로 다른 이미지들이 보여주지 못하는 다른 방법으로 데이터를 보여준다[6].

FloVis의 기본 화면(Bundle Diagrams)은 내부와 외부 네트워크상의 시스템들 간에 발생하는 NetFlow 연결을 보여주는데 초점을 둔다. 방사형의 원 테두리 상에 IP 주소와 함께 점으로 표시되는 각각의 시스템들 간의 데이터 흐름을 선으로 연결하는데 화면에 표시된 각 시스템을 클릭하면, 해당 시스템의 포트별 시간 변화와 그에 따른 데이터 흐름의 양을 보여주는 또 다른 시각화 화면(NetBytes Viewer)이 실행된다.

FloVis는 하나의 원 위에 관찰 대상 시스템들 간의 데이터 흐름을 표현하여 사용자가 네트워크의 상황을 한눈에 볼 수 있도록 해준다는 장점이 있다.

그러나 화면에 다수의 선의 연결로 표시되는 트래픽들을 해석하여 보안상 중요한 정보를 '식별'하는 과정이

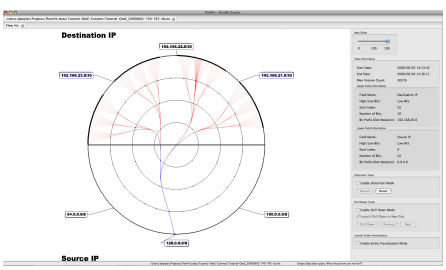

Fig. 3. FloVis

직관적이지 않으며, 대규모 네트워크상에서는 과도하게 많은 선들이 화면상에 표시되어 '식별'에 어려움이 발생하게 되는 단점을 가진다.

2.1.4 SecVis

SecVis는 네트워크 트래픽을 신속히 분석하기 위해서 2차원 또는 3차원의 화면상에 시간흐름에 따른 산점도(scatter plots)와 평행좌표그림(parallel coordinate plots)을 동적으로 표현하는 방법으로 시각화해준다[7].

SecVis는 사용자에게 네트워크 전체에 어떤 활동이 발생하는지를 한눈에 보여주면서 동시에 각 활동에 대한 상세 정보 제공 능력을 유지 하는 것을 목표로 디자인되었다. 입력 데이터로는 두 가지 형태가 사용 가능하며, 한 가지는 실시간 모니터링을 위한 라이브 패킷 캡처이고, 다른 하나는 포렌식을 위한 플레이백 모드에 사용되는 과거의 캡처된 데이터들이다.

Fig. 4.는 SecVis의 화면이며, 화면의 위아래를 가로지르는 두 개의 직선 중 왼쪽의 직선은 캡처된 패킷의 소스 IP 주소를 연속적으로 나타내며 화면 하단 끝이 0.0.0.0, 상단 끝이 255.255.255.255이다. 오른쪽의 직선은 목적지 포트 번호를 연속적으로 나타내며 하단 끝이 0, 상단 끝이 65,535이다. SecVis는 이러한 2개의 평행 직선을 연결하는 직선들의 형태로 특정 시점의 데이터 흐름을 보여준다. 이렇게 데이터 흐름이 표시되는 두 개의 직선 좌우측에는 수직선의 형태로 선의 높이에 따라 패킷의 크기를 보여주는 그래프가 표시되고 시간의 흐름에 따라 중심의 평행 직선으로부터 멀어지게 된다.

SecVis는 앞서 살펴본 또 다른 평행좌표축 기반의 시각화 도구인 VisFlowConnect와 같이 특정 시점의 네트워크 전체의 트래픽 흐름을 하나의 화면에서 한눈에 볼 수 있도록 하고, 또한 시간의 흐름에 따라 각 시스템의 패킷 량의 변화를 동일한 화면에서 동시에 관찰할 수 있도록 했다.

그러나 평행 축을 기반으로 화면에 표시되는 선들의 집합이 네트워크 전체의 상황을 식별하는데 직관적이지 않다. 특히 대규모 네트워크상에서는 트래픽을 나타내는 다수의 선들이 발생하여 '식별', 이 어려워지는 단점 또한 VisFlowConnect와 동일하다.

2.1.5 Visual Fingerprinting

Visual Fingerprinting은 흔히 사용되는 네트워크 스캐닝 툴 등의 공격 도구들이 동작할 때, 네트워크 트래픽들이 시각화되며 나타내는 특징들을 토대로, 각 공격에 이용된 공격 도구와 공격 방법을 구별하기 위하여 개발되었다[8].

이 도구는 시간의 흐름에 따른 네트워크상의 패킷 양과 접속 포트 등을 선의 길이와 점의 위치 등으로 표시하는 부수적인 시각화 화면을 제공하지만, 가장 핵심적인 화면은 앞서 살펴본 VisFlowConnect, SecVis 등과 같이 평행축을 기반으로 한 것이다.

이 화면에서 좌우로 평행하게 표시되는 각각의 축들에는 소스 IP, 목적지 IP, 소스 포트, 목적지 포트가 연속적으로 표시되며, 네트워크 트래픽은 각각의 평행축 상의 IP와 포트를 잇는 선으로 표시된다.

이 도구는 앞서 살펴본 다른 평행축 기반의 도구들과 같이 전체 네트워크의 데이터 흐름을 한눈에 볼 수 있다는 장점을 가지며, 기존 도구들과는 달리 각각의 평행축에 IP, 포트 등의 요소를 선택적으로 나타내어 다양한 형태의 시각화 패턴 표현과 분석이 가능하다는 장점을 함께 가진다.

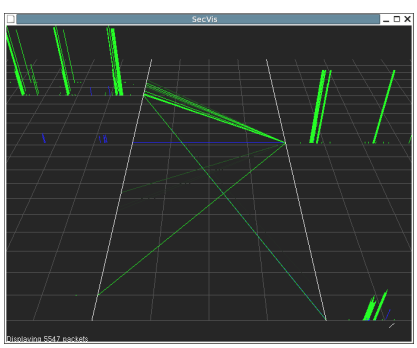

Fig. 4. SecVis

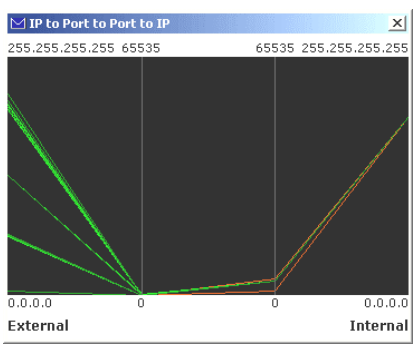

Fig. 5. Visual Fingerprinting

그러나 평행 축을 기반으로 화면에 표시되는 선들을 집합이 네트워크 전체의 상황을 식별하는데 직관적이지 않으며, 특히 대규모 네트워크상에서는 트래픽을 나타내는 다수의 선들이 발생하여 '식별', 이 어려워진다는 단점은 앞서 살펴본 다른 평행 축 기반의 시각화 도구들과 동일하다.

2.1.6 The Spinning Cube of Potential Doom

The Spinning Cube of Potential Doom(이하 'Cube'라 함)은 Bro Intrusion Detection System에서 수집된 네트워크 트래픽을 동적으로 보여주는 시각화 도구로서, 악의적인 트래픽의 수준을 네트워크 보안에 전문적 경험이 없는 사람도 쉽게 이해할 수 있도록 시각화해 보여준다[9].

Cube는 정보를 사용자가 마음대로 회전시킬 수 있는 3차원 정육면체의 형태로 보여주는 방법으로, 접속이 시도되거나 완료된 모든 TCP 연결을 기록하는 Bro IDS의 능력을 최대한으로 활용한다. Cube가 화면에 보여주는 3차원 정육면체의 각 축은 TCP 접속의 각 구성 요소를 나타내며, X축은 로컬 IP 주소, Z축은 global IP 주소, Y축은 접속에 이용된 포트 번호를 나타낸다. 그리고 모든 TCP 접속은 하나의 점으로 나타나며, 이중 성공한 접속은 흰색, 실패한 접속은 포트 번호에 따라 다른 여러 가지 색상으로 표시된다.

이상과 같은 Cube의 시각화는 하나의 3차원 정육면체 안에 전체 네트워크의 TCP 접속을 모두 시각화하여, 포트 스캔 등 이상 접속을 쉽게 '식별'할 수 있다는 장점을 가진다.

그러나 각각의 시스템들을 점의 형태로 표현해 '이해'에 필요한 정보들을 화면상에 함께 표현할 공간이 없다는 단점이 있다.

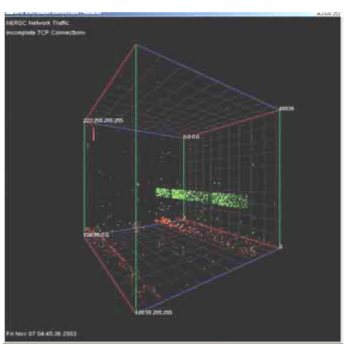

Fig. 6. The Spinning Cube of Potential Doom

2.2. 보안 경보 시각화 기술

2.2.1 IDS RainStorm

'IDS RainStorm'은 네트워크 전체의 IDS 경보 발생 상황을 실시간으로 한눈에 볼 수 있도록 해준다. IDS 경보 정보는 다수의 Y축 상에 표시되는 IP주소와 함께 표시되며, 상세한 정보를 얻기 위해 드릴다운(Drill down)할 수 있는 줌 기능을 제공한다. X축에 표시되는 시각은 경보의 패턴을 보여주기 위해서 사용되며, 색상의 변화를 이용해 경보의 심각성과 양을 나타낸다[10]. 기본 설정인 빨간색은 심각한 우려, 노란색은 중간 우려, 녹색은 낮은 우려를 나타내며, 이 설정은 사용자가 변경할 수 있다. 또한, 경보의 심각성 정도에 따라 IDS 경보를 필터링해 보여주는 기능도 있다.

'IDS RainStorm'는 최초 기본 화면에서 네트워크의 모든 IDS 경보 현황을 살펴볼 수 있고, 필요시 줌 기능을 통하여 더욱 상세한 정보를 얻을 수 있다.

그러나 기본적으로 네트워크상의 모든 시스템의 IDS 경보를 나타내기 때문에, 대규모 네트워크에서는 자체적인 필터링 기능을 이용하더라도 너무 많은 경보들이 화면상에 표시되며, 보안 정책상 중요한 경보를 적시에 '식별'하는데 어려움이 발생하게 된다.

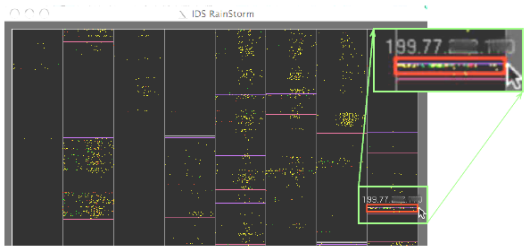

Fig. 7. IDS RainStorm

2.2.2 SnortView

SnortView는 관리자들이 IDS 경보들을 더욱 빠르고 쉽게 분석할 수 있도록 돕는 IDS 로그 시각화 시스템으로, 2차원의 다이어그램에 기반해 각각의 IDS 경보들을 포트번호, 프로토콜 등에 따라 다른 스타일과 색상의 아이콘들로 표현한다[11].

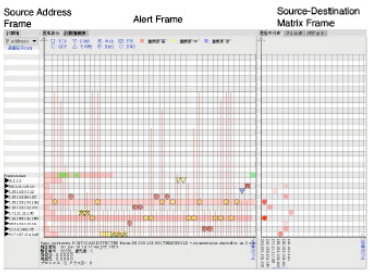

Fig. 8. SnortView

이 도구는 X축에 표시되는 시간의 변화에 따라 Y축에 표시되는 각 소스 IP들에서 발생되는 IDS 경보들을 시각화 해 네트워크 전체의 IDS 경보 발생 상황을 알려준다.

이 도구는 IDS 경보를 통신포트, 프로토콜 등의 차이에 따라 각각 다른 도형과 색상으로 표현하는 방법을 사용하여, 경보의 종류와 중요성 등을 한눈에 확인하고 보안 상황을 효과적으로 '식별'할 수 있다. 그러나 '이해' 단계를 돕기 위한 추가적인 정보 제공이 부족하다는 단점을 가지고 있다.

2.2.3 Avisa

Avisa는 방사형(radial) 시각화 패러다임을 토대로 만들어진 시각화 도구이다. 이 패러다임은 특정한 데이터가 원의 내부와 외부에 표현될 수 있도록 하며, 매우 컴팩트한 구조를 가진다[12].

Avisa는 방사형 패널과 내부 호(arc)라는 두 가지 주요 구성요소를 가진다. 방사형 패널은 '내부 원'(inner ring)과 '외부 원'(outer ring)으로 구성된다. 좌측 상단에 표시되고 '경보 유형 패널'이라 불리는 '내부 원' 내부의 색상 구분은 IDS 경보의 유형들을 보여준다. 이러한 색상 구분 바로 위에 위치하는 '외부 원'은 경고 유형들의 범주를 묶고, 사용자의 상호작용을 가능하게 하는데 사용된다. 각각의 경보 유형 범주에는 한 가지 색상이 사용되고, 해당 범주 내부의 각 경보 유형은 명암의 구분을 통해 세분화 한다.

방사형 패널 내부에 표시되는 호들은 실제 경보들을 표시한다. 전송중인 트래픽에 대하여 IDS가 발생시킨 경보들은 좌측 상단의 '경보 유형 패널'에서 시작하여, '내부 원' 중 '경보 유형 패널'을 제외한 나머지 부분인 '호스트 패널'에 표시되는 호스트 중 해당 경보와 관련된 것을 연결하는 호를 그린다.

Avisa는 전체 네트워크를 하나의 방사형 패널 내

Fig. 9. Avisa

에 표시하여, 한눈에 전체적인 네트워크의 상황을 살펴볼 수 있도록 하고, 경보의 범주와 해당 범주에 속하는 경보의 유형을 각각 색상과 명암의 차이로 표현하여 누구든지 쉽게 유형별 경보의 발생 상황을 '식별'할 수 있다는 장점이 있다.

그러나 다수의 보안 경보 발생시, 선들이 화면을 가득 채우게 되어 그 중 정책상 중요한 경보의 '식별'이 어렵게 되며, '이해'를 돕기 위한 추가적인 정보의 제공이 부족하다는 단점이 있다.

2.2.4 BANKSAFE

BANKSAFE는 대규모의 컴퓨터 네트워크에 대한 상황 인지를 위해 개발된 어플리케이션이다. 이 도구가 제공하는 Treemap Timestamp Snapshot 시각화(Fig. 10.)는 네트워크상의 수많은 컴퓨터들의 건강 상태 또는 정책 상태를 적시에 살펴볼 수 있도록 해준다[13].

화면을 구성하는 많은 사각형들의 크기는 각 네트워크 그룹에 존재하는 호스트들의 수에 비례하며, 이 사각형들의 색깔은 네트워크상 각 시스템들의 건강 상

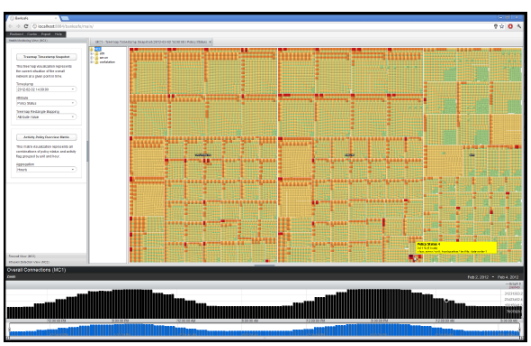

Fig. 10. BANKSAFE

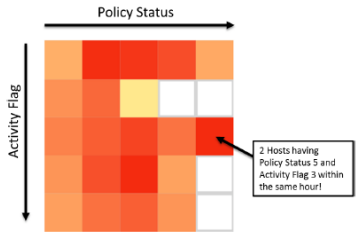

Fig. 11. 5×5 matrix of BANKSAFE

태나 정책 상태를 나타낸다. 또한 컴팩트하지만 높은 밀도의 정보 시각화를 제공하기 위해서, 픽셀 기반의 매트릭스를 추가적으로 제공한다. 이 5×5 색상의 매트릭스(Fig. 11.)는 특정한 시간 동안 한 개 네트워크 그룹에 가능한 모든 정책과 활동 점수의 조합에 해당하는 호스트들의 수를 색상으로 나타낸다.

이 도구는 공간의 낭비 없이 사각형의 배치하여 한 개의 화면에 매우 많은 호스트들을 한눈에 볼 수 있도록 시각화하고, 호스트들의 정책, 활동 상태를 색상의 차이로 쉽게 알 수 있도록 했다.

그러나 중요한 보안 이벤트가 발생한 시스템을 포함하여 모든 시스템들을 한 화면에 나타냄으로 인해, 위험 이벤트가 발생한 시스템들이 다른 시스템들 속에 가려져 효과적 '식별'이 어렵게 되는 문제점이 있으며, 이 문제점은 대규모의 네트워크상에서는 더욱 커지게 된다.

2.2.5 VisAlert

VisAlert는 여러 종류의 IDS 로그들에서 확인되는 다양한 네트워크 및 호스트 기반의 경보들 간의 상관관계에 대한 시각화 도구이다[14]. 이 도구는 화면 중앙에 로컬 네트워크의 토폴로지 맵을 표시하고, 외부를 둘러싸는 원들에는 다양한 경보 로그들(특정한 경보 유형에 따라 원을 분할)을 함께 보여준다. 원의 폭은 여러 기간으로 구분되는 시간대를 표시한다. 그리고 각각의 경보들은 경보 유형을 표시하는 외부의 원과 공격 대상인 로컬 노드를 연결하는 직선의 형태로 표시된다.

이 도구 또한 다른 방사형의 시각화 도구와 같이 전체 네트워크를 하나의 방사형 패널 내에 표시하여 한눈에 볼 수 있도록 하고, 외부 원 위의 각각 다른 위치에 표시되는 경보의 유형별로 각기 다른 색상을 부여하여 그 의미를 쉽게 파악할 수 있도록 하였다. 그러나 앞서 살펴본 Avisa와 동일하게, 다수의 보안 경보

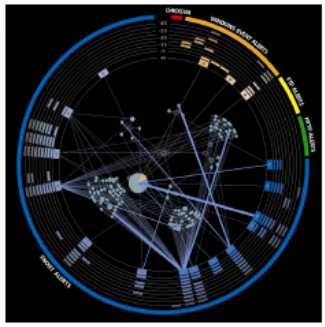

Fig. 12. VisAlert

발생 시 해당 선들이 화면을 가득 채우게 되어 그 중 정책상 중요한 경보의 '식별'이 어렵게 되고, '이해'를 돕기 위한 추가적인 정보의 제공이 부족하다는 단점을 가지고 있다. 방사형 구조 내부에 표시되는 네트워크상의 시스템들이 보안상 위험한 경보의 발생 여부와 관계없이 모두 표시됨으로 인해, 대규모 네트워크에서는 '식별'에 어려움을 발생시키게 된다.

2.2.6 IDSRadar

IDSRader는 방사형 그래프를 이용해 네트워크를 실시간으로 모니터링하고, 전체적인 보안상황을 감지할 수 있도록 해주는 IDS 경보 시각화 도구로서, ①서버와 워크스테이션, ②공격 유형, ③타임라인과 히스토그램, ④공격의 상호 관계, ⑤기타 정보를 나타내는 다섯 가지의 주요 영역들로 구성된다[15].

방사형 그래프 내부에 표시되는 서버, 워크스테이션 등 시스템과 원의 테두리 상에 표시되는 발생한 경보의 유형을 서로 연결하는 직선을 이용한 시각화 방법은 앞서 설명한 VisAlert와 동일하다.

그러나, 방사형 그래프의 테두리 내부에 표시되는

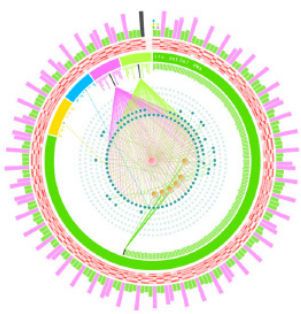

Fig. 13. IDSRader

히스토그램의 높이 변화를 이용해 시간대별 경보 횟수의 변화를 실시간으로 확인할 수 있게 했다. 만약 특정 시간대의 위험 이벤트 발생량 등을 토대로 위험하다고 판단된 경우, 방사형 그래프 외부에 적색 삼각형을 표시하여 사용자가 쉽게 위험 상황을 인지할 수 있도록 하는 등 VisAlert에 비하여 더욱 향상된 기능을 가지고 있다. 다만 VisAlert가 가진 '식별'에 대한 단점들을 동일하게 가지고 있다.

2.3 기존 연구의 장단점

이상과 같이 다양한 네트워크 보안 시각화 도구들에 대한 분석을 통해 '식별'과 '이해'의 측면에서 장·단점들을 파악하였으며, 이는 Table 1, 2와 같이 정리할 수 있다.

Table 1. summary of existing tools' advantages

tool	advantage
NVision IP	- Shows all network traffic flows in one screen - Provides stepwise visualization for more detailed informations
VisFlowConnect	- Shows all network traffic flows in one screen - Users can focus on particular traffic informations by using filtering function
FloVis	- Shows all network traffic flows in one radial panel
SecVis	- Shows all network traffic flows in one screen - Shows trend of each time period's traffic amount in one screen
Visual Finger printing	- Shows all network traffic flows in one screen - Can express and analyse various visualization patterns made by showing IP, port number and etc on each parallel axises
The Spinning Cube of Potential Doom	- Can identify anomalies easily by showing all TCP connections in one 3D cube
IDS Rain Storm	- Shows all IDS alerts in one screen - Provides 'zoom' function for more detailed informations
Snort View	- Effective in 'identification' and 'understanding' by virtue of expressing alert type and risk with figures and colors
Avisa	- Shows all network security alert status in one radial panel - Helps 'identification' by expressing each alert's category and type with difference of color and shade
BANK SAFE	- Shows many hosts in one screen by using rectangles without wasting space - Users can easily know each host's activity and policy status with difference of color
VisAlert	- Shows all network security alert status in one radial panel - Helps understanding each alert's meaning by difference of color
IDS Radar	- Shows all network security alert status in one radial panel - Helps understanding each alert's meaning by difference of color - Shows alerts count of each time period with histogram - Helps identifying and understanding big security risks with drawing red triangle

각 도구의 장점들을 모두 종합하면, ①하나의 화면에서 전체 네트워크의 상황을 관찰할 수 있도록 하여 '식별'에 도움을 주며, ②도형, 색상, 명암을 활용하여 '식별', '이해'를 쉽게 하고, ③기본 화면에 보여주는 정보를 최소화하여 '식별'을 효과적으로 하되, ④'이해' 단계를 위하여 필요시 더욱 상세한 정보를 얻을 수 있는 단계적 시각화를 제공한 점으로 요약된다.

그리고 각 도구들이 가진 단점들을 종합하면, ①보안상 중요한 이벤트의 발생 여부와 관계없이 네트워크 상의 모든 시스템들을 화면상에 표시하여 '식별'에 장애를 초래하고, ②트래픽, 경보 발생을 '선'을 형태로 나타냄으로 인해 '식별' 과정에 해당하는 선의 의미를 해석하는 과정이 필요하고, 특히 대규모 네트워크의 경우에는 과도하게 많은 선들이 화면을 채우게 되어 '식별'에 어려움을 발생시킨다. 그리고 ③시스템을 '점'의 형태로 표시하여 '이해'에 필요한 정보를 표시할 공간이 없으며, ④'이해'에 필요한 추가적인 정보의 제공이 부족하였다.

'허니컴'은 대규모 네트워크에 있어서 IDS, 방화벽 등의 보안 경보 이벤트 정보를 이용한 효과적 보안 상황 인지를 돕기 위한 시각화 시스템으로, 기존의 시각화 도구들이 '식별'과 '이해'에 있어 보여준 장점들을 최대한 활용·강화하고 단점들을 최대한 보완·해결할 수

Table 2. summary of existing tools' disadvantages

tool	disadvantage
NVision IP	- Has no space to show detailed information for 'understanding' due to drawing each system as a dot
VisFlowConnect	- Difficult to identify each meaning of lines connecting paralllel axises - Much traffic makes too many lines and 'Idetification' becomes hard
FloVis	- Difficult to identify each traffic shown as a line - Much traffic makes too many lines and 'Idetification' becomes hard
SecVis	- Difficult to identify each traffic shown as a line - Much traffic makes too many lines and 'Idetification' becomes hard
Visual Finger printing	- Difficult to identify each meaning of lines connecting paralllel axises - Much traffic makes too many lines and 'Idetification' becomes hard
The Spinning Cube of Potential Doom	- Has no space to show detailed information for 'understanding' due to drawing each system as a dot
IDS Rain Storm	- Many lines made by much traffic makes identifying important alerts hard
Snort View	- Lack of providing information to help 'understanding'
Avisa	- Many lines made by many alerts makes 'identification' difficult - Lack of providing information to help 'understanding'
BANK SAFE	- 'identification' is not effective due to showing all systems irrespective of having important events
VisAlert	- Many lines made by many alerts makes 'identification' difficult - Lack of providing information to help 'understanding' - 'identification' is not effective due to showing important alerts with common ones
IDS Radar	- Many lines made by many alerts makes 'identification' difficult - Lack of providing information to help 'understanding' - 'identification' is not effective due to showing important alerts with common ones

있도록 디자인되었다.

III. 허니컴(Honeycomb) 시각화 시스템

3.1 시각화 디자인 설계 방향

허니컴의 시각화 디자인 설계의 방향은 다음과 같다.

먼저 대규모 네트워크에서의 효과적 '식별'을 위하여, ①가능한 하나의 화면에서 전체 보안 상황을 관찰할 수 있도록 하되, ②기본 화면에서 보이는 시스템과 정보는 '식별'에 필요한 것만으로 최소화하고, ③ '식별'에 어려움을 줄 수 있는 '선(line)을 사용하지 않았다.

그리고 효과적 '이해'의 측면에서 ①단계적 시각화를 통하여 사용자의 필요 시 이해를 돕는 추가 정보를 제공하고, ②각각의 시스템을 '점'이 아닌 도형으로 표현하여 이해에 필요한 정보를 함께 나타낼 수 있도록 하였다.

마지막으로, '식별'과 '이해' 양 측면의 효과성을 모두 제고하기 위하여, 텍스트의 사용을 최대한 배제하고, 도형과 색상을 최대한 사용하였다.

3.2 시각화 디자인 설계상 특징

허니컴은 이상과 같은 설계 방향에 따라 ①벌집 구조 사용과 '선'의 생략, ②중요 이벤트가 발생한 목적지 중심의 시각화, ③표시 정보의 최소화와 세부 정보의 단계적 제공, ④색상의 활용이라는 네가지 특징을 가진다.

3.2.1 벌집 구조 사용과 '선'의 생략

네트워크의 관리자는 네트워크상에서 다수의 시스템 보안 상태 정보를 식별, 이해를 거쳐 보안 상황을 인지하게 된다. 본 연구에서는, 그 과정의 효과성을 제고하기 위해서 네트워크상의 수많은 시스템들과 그들의 상태를 하나의 화면에 단순화하여 모두 나타낼 수 있도록 하였다.

앞서 살펴본 대부분의 시각화 도구들은 하나의 화면에 모든 시스템들을 나타내기 위하여, 각각의 시스템들을 평행 축 또는 방사형 구조의 테두리 위에 표시되는 점의 형태로 표현하였다. 그러나 각각의 호스트를 점으로 표현할 경우에는 각 호스트의 상태를 식별, 이해하는데 필요한 최소한의 정보를 함께 표현할 공간이 없다는 단점이 있다.

이로 인해 기존의 시각화 도구들은 각 호스트에 발

생한 트래픽, 경보 등의 보안 이벤트 정보를 표현하기 위하여, 다른 시스템 또는 보안 경보 표시와 연결되는 선들을 화면에 표시하였다. 그 결과, '식별' 과정에서 해당 선의 의미를 해석하는 과정이 필요하게 된다. 특히 대규모의 네트워크에서는 보안 이벤트의 증가에 따라 수많은 선들이 화면을 가득 채우게 되어, 정작 중요한 정보를 적시에 식별하기 어려운 문제가 발생했다.

허니컴은 이러한 단점을 해결하기 위하여 네트워크 상의 시스템들을 각각 아래 Fig. 14.와 같은 하나의 정육각형으로 나타내었다. 정육각형은 여러 개체들을 나란히 배열할 경우, 모든 변들이 빈틈없이 서로 맞닿아 아래 Fig. 15.와 같은 벌집의 구조를 이루게 되어, 공간의 낭비 없이 많은 개체들을 나타낼 수 있다. 또한 정육각형 내부의 구분된 공간을 이용해 해당 호스트의 상황을 알려주는 필수 정보들을 시각화 할 수 있다는 장점을 가진다. 허니컴은 각각의 시스템을 나타내는 정육각형의 내부에 해당 시스템에 대한 정보들을 표시하여, 화면상에서 '선(line)'을 제거하였다.

Fig. 14. a hexagon structure used to describe a system

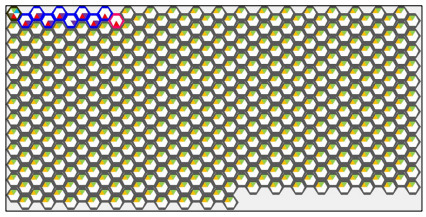

Fig. 15. a honeycomb structure made by describe many systems on a network

3.2.2 중요 이벤트가 발생한 목적지 중심 시각화

기존의 시각화 도구들은 보안 이벤트를 시각화할 때, 통상적으로 네트워크 내부의 모든 시스템들의 IP와 이벤트가 발생한 외부 시스템의 IP를 모두 나타낸 뒤, 각각의 이벤트는 소스 IP와 목적지 IP를 연결하는 선 또는 평면상 교차지점의 점의 형태로 보여주고 있다. 그러나 이러한 형태의 시각화는 대규모 네트워크의 경우 화면상에 너무 많은 시스템들을 나타내게 되어, 관리자의 확인이 필요한 시스템들이 다수의 시스템들 속에서 숨겨지게 되는 문제가 존재했다.

이러한 문제점을 해결하기 위해 허니컴은 기본적으로 중요한 보안 이벤트가 발생한 목적지 시스템만을 화면에 표시하는 방법으로, 화면상에 표시되는 시스템들의 수를 최소화하고, 사용자로 하여금 이벤트가 발생한 시스템을 쉽게 발견할 수 있도록 하였다.

통상적으로 침해의 중요성을 판단할 때, 우선적으로 위험 이벤트가 발생한 목적지를 먼저 확인하고, 그 뒤에 해당 이벤트를 발생시킨 시작점(소스 IP)를 확인하는 것이 일반적[16]이기 때문이다. 기본 화면에서는 목적지 시스템 중심의 시각화 화면을 구현했으며 사용자의 필요시에는 추가적인 시각화 화면을 통해, 각각의 목적지 시스템과 관련된 소스 IP 시스템 등의 정보를 확인할 수 있다.

3.2.3 표시 정보의 최소화와 세부 정보의 단계적 제공

대규모 네트워크의 관리자들에게는, 보안상황인지를 위한 '식별'의 단계, 즉, 다량의 보안 정보 중에서 정말 필요한 정보를 적시에 찾아내는 것은 쉽지 않은 작업이다. 이러한 '식별' 단계를 효과적으로 돕기 위한 시각화 도구는 필요한 정보만을 최소화하는 것이 필요하다.

이를 위해 '허니컴'은 네트워크의 보안 정책에 따라 가장 중요한 보안 정보들의 유형을 사용자가 사전에 설정하고, 그 설정에 따라 시각화된 화면을 제공하여, 사용자가 정말 중요 정보들에 집중할 수 있도록 하였다.

그러나 '표시 정보의 최소화'는 이어지는 '이해'의 과정에서 필요한 정보를 생략하여 어려움을 발생시킬 수 있어, 시각화의 단계 구분을 통해 필요시에는 세부 정보를 얻을 수 있도록 하여 '이해' 단계를 도울 필요가 있다.

이를 위해 허니컴은 '식별'과 '이해'를 위한 화면을 각각 제공한다. 네트워크 관리자가 통상적으로 모니터링하는 기본 화면(1단계)상에서는 보안 이벤트의 '식별'에 초점을 맞추어 필요 최소한의 정보를 제공한다. 이상 이벤트 발견시 '이해'의 과정에 필요한 더욱 세부적인 정보를 담은 시각화 화면을 단계적으로 확인할 수 있다.

3.2.4 텍스트의 최소화와 이미지의 사용

이미지는 사용자에게 즉각적으로 인지되기 때문에 큰 노력 없이도 텍스트보다 빠르게 정보를 전달할 수 있다[17].

허니컴은 네트워크 보안상황에 대한 더욱 효과적인 '식별'과 '이해'를 위해, 텍스트 사용을 최대한 줄이고, 보안 경보가 발생한 시스템의 경보 유형을 여러 가지 색상의 도형으로 표현하였으며, 전체 네트워크의 보안 상황이 벌집 형태의 한 이미지로 보이게 하였다.

3.3 세부 인터페이스

3.3.1 Main View (1단계)

허니컴의 Main View는 ①IDS, 방화벽에서 사용자가 설정한 중요 보안 이벤트의 발생한 시스템들의 현황을 벌집의 형태로 보여주는 '노드 테이블'(Node Table), ②분석 대상 시간대의 시작과 끝을 정할 수 있는 '시간 입력 컨트롤'(Time Input Control), ③네트워크 보안 정책 등을 토대로 사용자가 사전에 설정한 5가지의 중요한 보안 이벤트를 보여주는 '이벤트 설정 뷰'(Event Setting View), ④설정된 분석 대상 시간대 동안 시간의 흐름에 따른 IDS, 방화벽의 탐지 건수의 추이를 그래프로 나타내어 보안 트랜드의 변화를 알려주는 '타임바'(Time Bar)[1]로 구성된다.

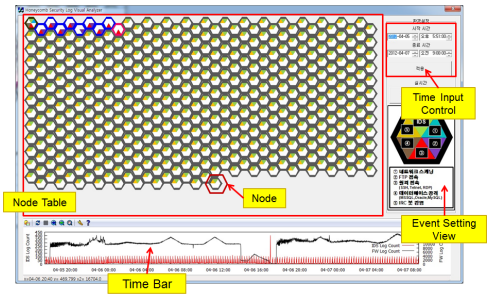

Fig. 16. Main View

3.3.2 노드 테이블(Node Table)

IDS, 방화벽에서 사용자가 설정한 5가지 중요 보안 이벤트가 발생한 시스템들의 현황을 벌집의 형태로 보여주는 곳이다. 중요 보안 이벤트가 발생한 경우, 해당 이벤트와 관련된 소스 IP, 목적지 IP 중 목적지 IP의 시스템만을 화면상에 1개의 정육각형으로 나타내며, 이러한 정육각형이 연속적으로 표시되어 벌집의 형태로 보이게 된다.

앞서 설명한 바와 같이 허니컴은 보안 이벤트가 발생한 각각의 목적지 시스템만을 나타내고, 소스 IP 시스템의 표현을 생략하고, 소스 IP, 목적지 IP간의 관계 표현을 위해 사용되는 '선'을 생략하여, 보안 이벤트가 발생한 시스템이 더욱 쉽게 '식별'된다.

화면상에 정육각형으로 나타나는 각각의 시스템들을 클릭하면, 그 시스템과 연결되어 중요 보안 이벤트를 발생시킨 소스 IP의 시스템들의 정보 등을 포함한 Connection View를 화면에서 확인할 수 있어 '이해' 과정을 위한 추가적인 정보를 얻을 수 있다.

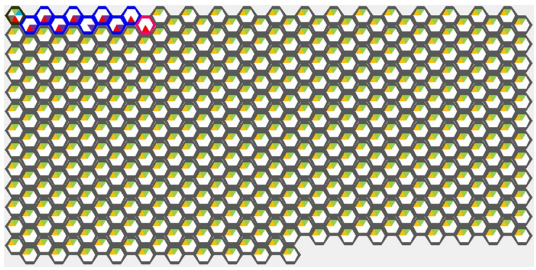

Fig. 17. Node Table

3.3.3 노드(Node)

노드 테이블에 표시되는 정육각형 모양의 노드들은 각각 중요 보안 이벤트가 발생한 하나의 시스템을 나타낸다. 노드는 네트워크 관리 주체가 설정한 중요하거나 위험성이 큰 다섯 가지 이벤트들의 발생 여부를 노드 내부를 구성하는 여러 가지 색상의 삼각형들의 유무로 표시하며, 이 중 상단의 삼각형은 IDS 경보의 탐지 여부를 나타낸다.

아래 Figure 18은 노드의 표시 형태를 보여주는데, ①, ②, ③, ④, ⑤의 삼각형들은 각각 중요 보안 이

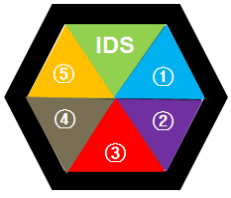

Fig. 18. Node

1) 오픈소스인 GNU Plot 4.6버전을 이용해 구현

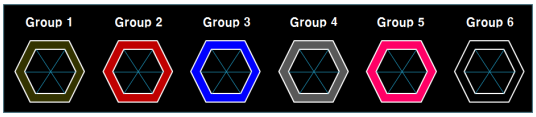

Fig. 19. different colors for each system groups (example)

벤트의 유무를 색상으로 보여주며, IDS가 표시된 삼각형은 해당 시스템의 IDS 탐지 여부를 나타낸다.

노드의 외부 테두리는 각 노드가 속한 시스템 그룹을 색상으로 표시하도록 하였다. 각 시스템 그룹별로 다른 색상을 부여하고, 특히 침해사고에 대한 위험성, 중요성이 높은 그룹에 대해서는 보다 눈에 잘 띄는 색상을 부여하여 '식별'에 용이하도록 설정할 수 있다.

3.3.4 Connection View (2단계)

Main View의 노드 프레임 상에 표시된 중요 이벤트가 발생한 노드들 중 하나를 선택하면, Fig. 20.과 같은 Connection View가 표시되며, '이해', '예측'의 단계를 위해 필요한 더욱 구체적인 정보를 보안 담당자에게 제공한다.

Connection View는 중요 보안 이벤트가 발생한 Main View상의 목적지 시스템과 연결되어 이벤트가 발생한 소스 IP 시스템들을 Main View와 같은 형태의 노드 프레임 상에 모두 표시해주고, 특히 유형별 이벤트가 가장 많이 발생한 소스 IP의 주소와 발생 횟수를 보여준다.

Connection View의 노드 테이블에도 Main View의 노드 테이블과 마찬가지로 해당 노드의 IP 정보가 기본적으로 표시되어 있지 않으며, 마우스를 클릭해서 확인할 수 있다.

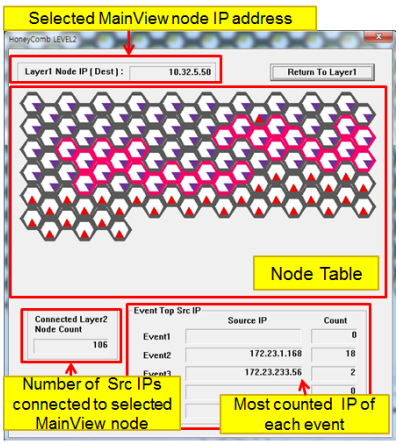

Fig. 20. Connection View

IV. 모의 테스트 결과 및 분석

4.1 테스트에 사용된 데이터

허니컴 시각화 시스템의 효용성을 실증적으로 확인하고자 모의 테스트를 수행하였다. 허니컴이 대규모 네트워크 시스템의 보안상황인지에 있어서 '식별', '이해' 과정에 가지는 효용성을 확인하기 위해서는 대규모 네트워크의 보안 경보 이벤트 정보가 필요하였으며, 그로 인해 테스트 과정에는 IEEE VAST 2012 미니 챌린지 2의 테스트 데이터가 사용되었다.[2)]

이 데이터는 Bank of Money(이하 BOM)라는 가칭의 은행 전산망의 방화벽과 IDS 장비에서 생성된 로그 데이터로, BOM의 네트워크는 약 4,000대의 workstation과 1,000대의 서버로 구성되어 있다. 또한, 일부 금융 거래들은 지역 은행 내부 네트워크의 금융 서버 상에서 이루어지며, 나머지 거래들은 기업 본부 데이터센터로 보내어진다.

이 데이터에 포함된 방화벽, IDS 로그의 생성 시기는 2012. 4. 5. 17:51부터 2012. 4. 7. 09:00까지로, 동기간의 방화벽 로그 생성 건수는 모두 23,711,341건(약4.09GB)이고, IDS 로그는 모두 51,073건(약21.81MB)이다.

4.2 BOM의 네트워크 보안 정책 및 중요 이벤트 선정

모의 테스트 과정에서 허니컴 시각화 시스템을 이용해 감시할 다섯 가지 중요 보안 이벤트를 선정하기 위해, 테스트 데이터와 함께 주어진 BOM의 네트워크 보안 정책[3)]을 살펴보았으며, 그 내용은 다음과 같다.

허용 가능한 사용 정책

아래의 내용들은 Bank of Money(BOM) 네트워크의 허용 가능한 사용 범위에 대한 정책이다. 모든 사원들은 이 정책에 관한 훈련을 받았다.

1. BOM 컴퓨터 네트워크는 오로지 업무 목적으로만 사용된다. 개인적인 용도의 회사 컴퓨팅 자원 사용은 금지되어 있다. **사원들은 개인적인 이메일, 소셜 네트워**

2) http://www.vacommunity.org/VAST+Challenge+2012
3) http://www.vacommunity.org/dl336

크, 경매 사이트 또는 개인적인 은행 활동 등을 위해서 회사 컴퓨터를 사용하면 안된다.

2. **사원들은 BOM 인트라넷을 집 등의 원격지에서 접속할 수 없다. FTP, Telnet, 원격 로그인, 원격 데스크톱 연결 등 BOM 인트라넷에 대한 모든 원격 접속은 차단되어 있다.**
3. BOM이 구입하고 소유하지 않은 USB 메모리 등의 외부 저장 매체는 회사 컴퓨터에서 사용될 수 없다. 회사 자산으로부터 제거된 회사 소유의 USB 메모리와 외부 저장매체들은 회사 자산들에 반환될 때 반드시 시스템 관리자로부터 검색을 받아 한다.
4. **BOM 네트워크상에서는 어떠한 개인 소유의 컴퓨터, 디바이스들도 사용되어서는 안된다.**
5. 회사가 구입하고 승인한 소프트웨어들만 BOM의 컴퓨터들에 설치될 수 있다. 소프트웨어들은 반드시 시스템 관리자가 설치하여야 한다. **파일 공유 프로그램과 P2P 통신 프로그램들은 BOM 컴퓨터 상에서 절대 허용되지 않는다.**

이상과 같은 정책에 따라, Table 3.과 같이 다섯 가지의 이벤트가 BOM의 네트워크 보안에 있어서 중요한 위험 징후가 될 수 있다고 판단하였다.

이 5가지 중요 이벤트의 발생 여부는 아래 Fig. 21.과 같이 노드의 내부를 채우는 각각 다른 색상을 가진 삼각형들의 표시 여부로 나타내며, 노드 상단의 삼각형은 IDS 경보 발생 여부를 나타낸다.

또한, BOM의 네트워크를 구성하는 방화벽, 재정 서버, 웹PC, 워크스테이션 등 시스템들의 그룹을 중요도에 따라 구분하고 각각 식별하기 용이하도록 노드

Table 3. 5 important events

No.	Event	Src.	Detection Rule
1	attempted information leak	IDS Log	class field is “Attempted Information Leak”
2	FTP connection	F/W Log	Destination port number is 21
3	remote login	F/W Log	Destination port number is 22, 23 or 3389
4	database attack	IDS Log	Label field includes “Suspicious inbound to” and “SQL”
5	IRC connection authorization	IDS Log	Label field includes “IRC authorization message”

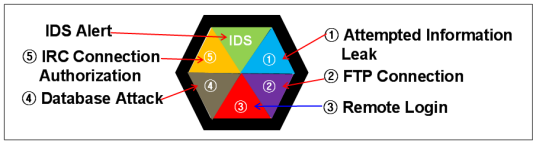

Fig. 21. 5 important events on a node

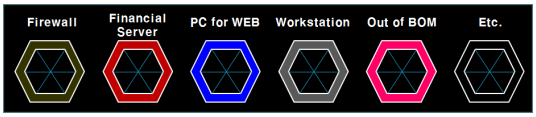

Fig. 22. colors of system groups

에 표시할 테두리 색상을 Fig. 22.와 같이 부여하였다.

4.3 중요 이벤트 시각화 및 탐지 결과

4.3.1 event1(attempted information leak), event4 (database attack)

전체 기간 동안의 데이터를 이용해 Main View 상에 중요 이벤트를 시각화한 결과는 아래 Fig. 23.과 같다. 설정된 5가지 중요 이벤트 중 1번 ‘attempted information leak’와 4번 ‘database attack’은 노드 프레임의 가장 왼쪽 최상단에 표시된 단 한 개의 방화벽(F/W) 서버에서만 탐지되었음이 확인된다.

이때 이벤트가 발생한 노드를 클릭하면, Connection View를 통해, 해당 노드의 IP 주소, 분석 대상 기간 동안 중요 이벤트를 발생시킨 모든 소스 IP의 현황과 발생한 이벤트의 종류가 아래 Fig. 24.와 같이 화면 상에 표시된다.

이벤트 1번과 4번 모두 5개의 소스 IP 시스템으로부터 위 방화벽 서버를 목적지로 하여 발생하였으며, 그 중 4개는 BOM 전산망 내부의 PC이고, 1개는 분홍색 테두리의 BOM 전산망 외부의 시스템임을 쉽게 확인할 수 있다.

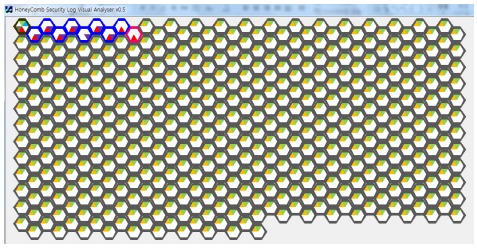

Fig. 23. visualization result of whole data

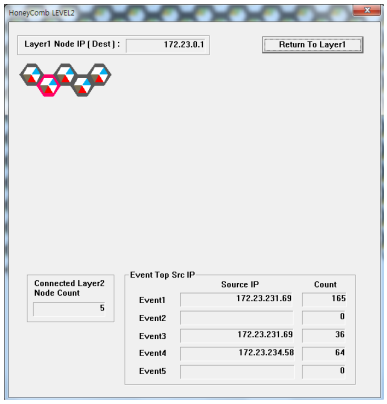

Fig. 24. Connection View (event 1,4)

4.3.2 event2(FTP connection)

Fig. 23.의 전체 시각화 결과를 보면, 파란색 테두리의 웹PC 7개에 FTP 접속이 이루어졌음을 알 수 있다. 이들 웹PC 들은 모두 아래 Connection View와 같이 회색 테두리의 내부 업무용 PC는 물론, 분홍색 테두리의 외부 시스템으로부터 FTP 접속이 이루어지고 있음이 확인된다.

그러나, BOM의 네트워크 정책상 회사 내부의 시스템에 외부로부터의 원격 접속은 차단되어 있다. 따라서 관리자는 외부로부터 화면상에 나타난 웹 PC들을 목적지로 하는 FTP 접속이 발생하는 원인을 확인하여, 침해 사고의 발생 여부를 확인해야 할 것이다.

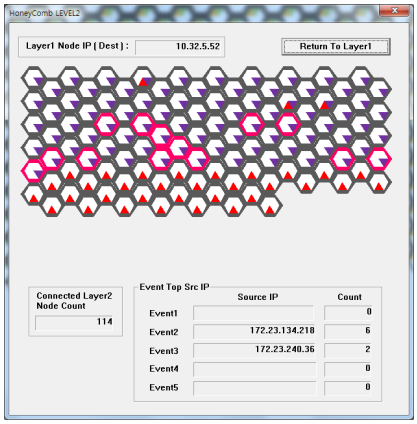

Fig. 25. Connection View (event 2)

4.3.3 event3(remote login)

Fig. 23.의 전체 시각화 결과를 보면, 이벤트 3번 '원격 로그인'이 발생한 목적지 시스템들은 모두 9개가 확인된다. 그 중 8개는 파란색 테두리의 웹 PC이고, 1개는 분홍색 테두리의 BOM 외부 시스템이다.

특히, 분홍색 테두리의 시스템은 BOM의 네트워크 정책을 위반하여, 전산망 내부에서 외부로 원격 접속이 이루어졌음을 나타내는 것으로 그 위험성이 매우 크다. 그리고 Connection View을 이용해 이 외부 시스템으로 접속한 내부의 소스 IP를 확인한 결과, IP는 10.32.0.100이며 검은색 테두리의 방화벽으로 확인된다.

즉, BOM 내부의 방화벽 시스템이 외부의 시스템으로 원격 로그인을 한 것으로, 보안 관리자는 신속히 원인을 파악하여, 침입의 여부를 판단하고 대응해야만 할 것이다.

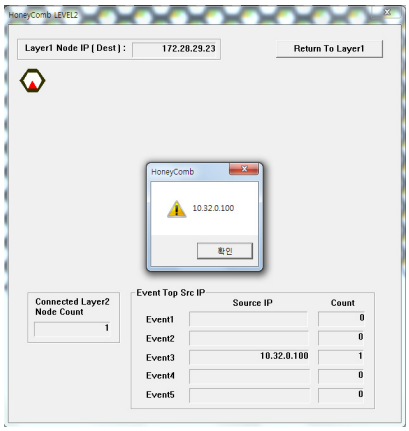

Fig. 26. Connection View (event 3)

4.3.4 event5(IRC Connection Authorization)

BOM의 네트워크 보안 정책상 IRC와 같은 P2P 통신 프로그램의 사용은 엄격히 제한되어 있고, 사원들 모두 이러한 보안 정책에 대하여 교육을 받았다.

그럼에도 불구하고 BOM 네트워크상에서의 IRC 통신은 Fig. 27.과 같이 2012.04.05. 20:00까지는 전혀 탐지되지 않다가 이후 Fig. 28.과 같이 워크스테이션을 중심으로 급증하였음이 확인된다.

이러한 IRC 통신량의 증가를 사원 개개인의 보안

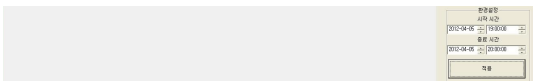

Fig. 27. 2012.04.05. 19:00 ~ 20:00 : No IRC connection was detected

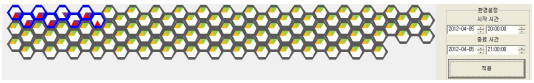

Fig. 28. 2012.04.05. 20:00~21:00: IRC connections to workstations suddenly increased

정책 위반으로 보기에는 단시간 동안의 증가량이 과도하게 크며, 따라서 위 시각을 전후하여 다수의 워크스테이션들에 IRC 통신을 하는 악성 프로그램의 감염이 확산된 것으로 강하게 의심된다.

V. 결론 및 향후과제

5.1 결론

본고에서 새롭게 디자인 한 '허니컴' 시각화 시스템은 대규모 네트워크에서 보안상황인지의 '식별', '이해', '예측' 단계 중 '식별'과 '이해'를 효과적으로 할 수 있도록 돕기 위해 제안하였다. '허니컴'은 기존의 네트워크 보안 시각화의 '식별'과 '이해'에 있어 가지는 장점을 극대화하고 단점을 극복하기 위하여 ①벌집 구조의 사용 및 '선'의 생략, ②목적지 중심의 시각화, ③표시 정보의 최소화와 세부 정보의 단계적 제공, ④텍스트의 최소화와 이미지의 사용이라는 특징을 바탕으로 설계되었다.

대규모 네트워크의 보안상황인지에 있어 '허니컴'이 제공하는 시각화의 효과성을 모의 테스트 해 확인한 결과, BOM의 대규모의 네트워크상에서 각각의 시스템들에 발생한 중요 이벤트의 현황을 효과적으로 식별·이해하고 보안상황을 인지하여 적절한 대응을 할 수 있도록 도와줄 수 있음을 확인하였다.

5.2 향후 과제

'허니컴'이 목적지 IP만을 기준으로 나타내는 것은 효과적 '식별'에 있어서 분명한 장점이지만, 소스 IP 중에서도 중요한 것은 지속적으로 관찰할 필요가 있다. 따라서 기본적으로 목적지 IP를 중심으로 각각의 노드들을 표현하되, 일부 소스 IP의 시스템들도 이벤트 발생 시 함께 보여줄 수 있도록 개선할 수 있을 것이다.

또한 이 도구는 사전에 설정한 5가지의 중요 보안 이벤트에 대한 '식별'과 '이해'에 초점을 두고 설계되었다. 그 결과 분석 과정에 필요한 다른 정보들을 충분히 제공하지 않아, 다른 도구를 이용한 정보 수집, 분석이 필요하다. 따라서 세부 분석 과정에서 더욱 상세한 정보들을 제공할 수 있도록 보완할 필요가 있다.

마지막으로, 중요 이벤트가 발생한 노드의 개수가 화면에 표현할 수 있는 범위를 넘어설 경우, 표현이 불가능하다. 따라서 그러한 경우를 대비해 화면에 표시되는 정육각형의 노드들의 크기를 사용자의 필요에 따라 확대, 축소할 수 있도록 개선하여 더욱 많은 노드들을 표현할 수 있도록 해야 할 것이다.

References

[1] Mica R. Endsley. "Toward a Theory of Situation Awareness in Dynamic Systems," Human Factors, 37(1), pp. 32-64. Mar. 1995.

[2] 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.

[3] Jang Beom-Hwan, Na Jung-Chan and Jang Jong-Su, "Security Situational Awareness technique using security event visualization" Review of KIISC / v.16, no.2, pp. 18-25, Apr. 2006.

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

[5] 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

[6] T. Taylor, D. Paterson, J. Glanfield and et al., "Flovis: Flow visualization system," Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology, pp. 186-198, Mar. 2009.

[7] 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.

[8] G. Conti and K. Abdullah, "Passive Visual Fingerprinting of Network Attack Tools," Proc. of VizSEC'04, pp. 45-54, Oct. 2004.

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

[10] A. Kulsoom, L. Chris, C. Gregory, A. C. John and S. John, "IDS RainStorm: visualizing IDS alarms," IEEE Workshop on Visualization for Computer Security, pp. 1-10, Oct. 2005.

[11] K. Hideki and O. Kazuhiro, "SnortView: visualization system of snort logs," The 2004 ACM work-shop on Visualization and data mining for computer security, pp. 143-147, Oct. 2004.

[12] S. Hadi, S. Ali and A. G. Ali, "IDS alert visualization and monitoring through heuristic host selection," ICICS'10 Proceedings of the 12th international conference on Information and communications security, vol. 6476, pp. 445-458, 2010.

[13] J. Fuchs, D. A. Keim, F. Mansmann and et al., "BANKSAFE: A visual situational awareness tool for large-scale computer networks: VAST 2012 challenge award: Outstanding comprehensive submission, including multiple vizes," Proceedings of the 2012 IEEE Conference on Visual Analytics Science and Technology, pp. 257-258, Oct. 2012.

[14] Yarden Livnat, Jim Agutter, Shaun Moon, Robert F. Erbacher and Stefano Foresti, "A visualization paradigm for network intrusion detection," Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC, pp. 92 - 99, Jun. 2005.

[15] Y. Zhao, F. F. Zhou and X. P. Fan, "a real-time visualization framework for IDS alerts," VINCI '12 Proceedings of the 5th International Symposium on Visual Information Communication and Interaction, pp. 11-17, 2012.

[16] K. Hideki and O. Kazuhiro, "SnortView: visualization system of snort logs," The 2004 ACM work-shop on Visualization and data mining for computer security, pp. 143-147, 2004.

[17] M. L. Fadel and C. M. Dyson, "Comparing a Text-and Visual-based Interface Presenting Social Information in an Online Environment," Visual Languages and Human-Centric Computing, pp. 143-146, Sep. 2006.

〈저자소개〉

박 재 범 (Jaebeom Park) 정회원
2002년 3월: 경찰대학교 행정학과 졸업
2012년 2월~2014년 5월: 경찰청 사이버테러대응센터 사이버테러수사팀 근무
2013년 9월~현재: 고려대학교 공공보안정책학과 석사과정
〈관심분야〉 정보보호, 디지털포렌식

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월~현재: 고려대학교 정보보대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌식

김 은 진 (Eunjin Kim) 정회원
1999년 2월: KAIST 산업경영학과 졸업
2001년 2월: KAIST 경영공학과 석사 졸업
2007년 8월: KAIST 경영공학과 박사 졸업
2008년 9월~현재: 경기대학교 국제산업정보학과 부교수
〈관심분야〉 경영정보시스템, 보안경제학