효과적 보안상황 분석을 위한 보안이벤트 처리

Security Event Processing for Effective Security Situation Analysis

u-IT839의 정보보호 이슈 특집

이수형 (S.H. Lee) 능동보안기술연구팀 선임연구원
방효찬 (H.C. Bang) 능동보안기술연구팀 선임연구원
장범환 (B.H. Chang) 능동보안기술연구팀 선임연구원
나중찬 (J.C. Na) 능동보안기술연구팀 팀장

목 차

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 해당 공격에 대한 적절한 대응을 수행하여야 하며 이를 위해서는 관리 도메인 상에서 발생하는 보안 이벤트들을 분석하여 현재의 보안 상황에 대한 파악이 필수적으로 이루어져야 한다. 본 논문에서는 보안상황 분석을 위해 보안이벤트간 연관성 분석 기술에 대한 일반적 동향과 이벤트 연관성 분석의 특정 분야로써 현재 활발이 연구가 진행중인 이벤트의 시각화를 통한 보안상황 분석에 대한 연구 동향을 다루도록 한다.

Ⅰ. 서론

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 웜 확산에 따른 인터넷 마비 사고에서처럼 네트워크 자체의 운용이나 성능에 영향을 미치고 결과적으로는 네트워크 서비스 제공 자체를 위협하는 단계에 이르렀다. 따라서 효과적인 네트워크 보안을 강구하기 위해서는 관리 대상이 되는 도메인에서 이루어지고 있는 공격에 대한 탐지와 그에 따른 단순한 공격 정보뿐만 아니라 그 공격으로 인한 피해의 정도와 범위, 탐지 이벤트의 신뢰성 문제, 또는 간접적 이벤트 분석을 통한 공격의 사전 탐지와 같은 보안 상황에 대한 분석 기술이 반드시 필요하다.

과거 보안 상황 분석 기술에는 이벤트 특성에 따른 분류로써 침입탐지시스템이나 방화벽 등에서 수집한 이벤트를 분석하여 침입 또는 공격이 있었는가를 판단하는 것과 네트워크의 패킷(트래픽)을 분석하여 트래픽의 이상 상태 여부를 판단하는 것이 주를 이루었으며, 분석 방법에 따른 분류로써는 로그 기록을 분석하여 공격자의 시그니처(signatures)를 찾는 오용탐지(misuse detection)와 정상적인 행동을 기반으로 비정상적인 행동을 찾는 비정상행위 탐지(anomaly-behavior detection)가 있다. 하지만, 이와 같은 방법들은 최근 폭발적인 이벤트 양과 오탐율(false positives) 때문에 신속성을 요구하는 공격(zero-day attacks)의 분석과 알려지지 않은 공격 등을 판별하는 데 있어서 많은 문제점을 드러내고 있다. 또한, 관리자들은 대량의 발생 이벤트로 인해 단순히 이벤트 정보만을 분석해서는 관리 대상 도메인 네트워크 내에서의 보안 상황을 인식할 수 있을 가능성은 전무한 상태이다.

따라서 대량의 보안이벤트 상호간의 연관성 분석을 통해 공격에 대한 정보와 보안상황에 대한 정보를 좀 더 축약적이고 지식화하여 관리자에게 제공함으로써 관리의 용이성을 증가시키고자 하는 노력이 활발히 진행중이다. 본 논문에서는 보안상황 분석을 위한 보안이벤트 연관성 분석 기술에 대한 일반적 동향과 보안이벤트 연관성 분석의 특정 분야로써 현재 활발이 연구가 진행중인 이벤트의 시각화를 통한 보안상황 분석에 대한 연구 동향을 다루도록 한다.

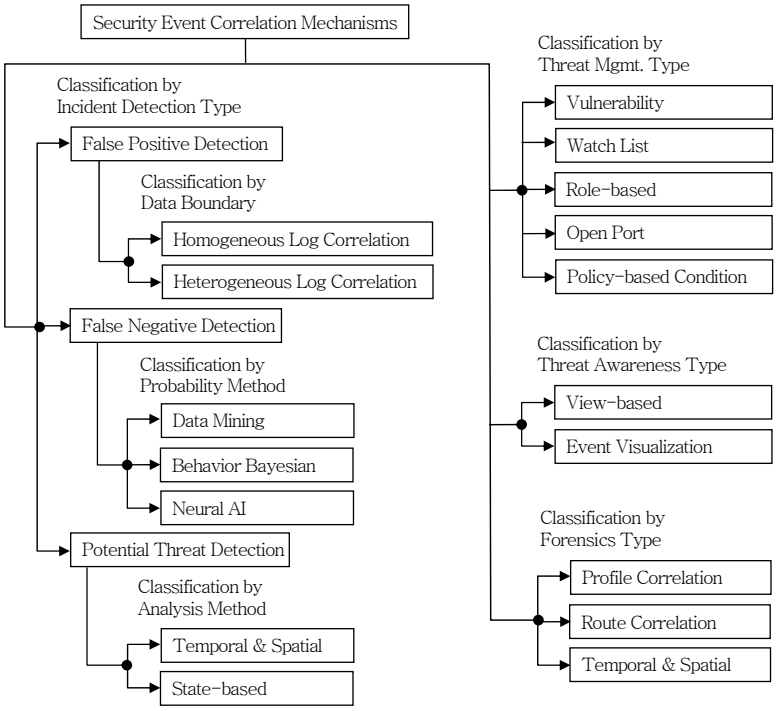
Ⅱ. 보안이벤트 연관성 분석

이벤트 연관성 분석 기술은 처음에는 네트워크 관리 분야에서 다양한 형태로 연구, 개발되어 왔으나 최근에는 네트워크 보안 관리 분야에서도 커다란 이슈가 되고 있다. 보안이벤트 연관성 분석 기술이 급증하고 있는 네트워크 보안에 관련된 대량의 이벤트 정보를 운용자가 수작업으로 처리할 수 없는 문제를 해결하기 위한 정보 관리 기술로서 또 한편으로는 독립적으로 발생한 다수의 이벤트 정보 간의 연관 관계를 분석함으로써 보안 침해 사건의 근본적인 원인을 규명하기 위한 지식 창조 프로세스로서 적용되고 있는 상황이다. (그림 1)은 보안 분야에서

● 용 어 해 설 ●

연관성 분석: 보안 침해 사건의 경우 일반적으로 공격이 이루어지기 전의 사전 작업 단계, 공격 실행 단계, 공격 후 피해 파급 단계 등으로 이루어지며 각 단계별로 다수 개의 네트워크 영역 및 시스템이 관련된다. 따라서 이들에서 발생하는 이벤트들간의 위치적, 시간적 상관관계를 분석함으로써 개별 이벤트들이 제공하는 사전 정보에서 발전된 도메인 상의 보안상황 지식을 생성하고자 하는 것이 그 목적이다.

보안상황: 보안 관리를 수행할 도메인의 보안 상태를 의미하는 말로 좁게는 관리 도메인상에 발생한 공격의 탐지와 그와 관련된 보안이벤트 데이터의 분석 결과를 의미하며, 넓게는 관리 도메인 상에 발생하는 각종 이벤트들을 분석하여 잠재적 위협 및 서비스 안정성을 침해할 수 있는 이상상태에 대한 분석 결과를 의미한다.



(그림 1) 보안이벤트 연관성 분석 기술 적용 분야

보안이벤트 연관성 분석 기술을 적용하기 위한 영역별로 그 분야를 나타낸 것이다.

1. 보안침해사건 탐지 영역

보안침해사건 탐지 영역에서 이루어지고 있는 연구들은 주로 보안이벤트 연관성 분석의 목적이 되는 네트워크 보안 탐지 영역, 즉 탐지하고자 하는 대상이 무엇인가에 치중하여 연구를 진행하고 있는 그룹이다. 즉 연관성 분석에 의한 오탐지율 제거를 위한 연관성 분석과 미탐지율(false negative) 보완을 위한 연관성 분석, 잠재적 위협(potential threat)을 탐지하기 위한 연관성 분석 기술 연구들이 그 대상이다[1],[2].

침입 탐지 시그니처 기반으로 동작하는 IDS는 매우 높은 오탐지 가능성을 갖는다. 사전 정의된 룰에 기반하여 탐지를 수행하기 때문에 약간의 오차에도 반응하는 false positive와 룰에 정의되지 않은 새로운 패턴에 대한 공격에는 반응할 수 없는 false negative가 양존한다. 또한, 네트워크 경계의 일정 위치에서만 패킷을 모니터링하는 특성 때문에 분산된 루트를 이용한 지능적인 공격은 탐지해 낼 수가 없다. 따라서 여러 IDS, F/W 등에서 발생하는 다양한 이벤트간의 연관성을 분석하여 IDS의 오탐지나 미탐지를 줄임으로써 탐지 효율을 높이려는 연구 분야가 있다. 이와 더불어 아직 공격이 수행중인 과정 속에서 잠재적인 위협을 내포하고 있는 potential threat을 탐지하기 위한 연구도 진행되고 있다.

가. 오탐지율 감소

False positive 관점에서의 오탐지율 제거를 위한 연관성 분석 방법은 한정된 단일 로그 정보만을 이용하여 네크워크에 대한 보안 침해 여부를 탐지하는 경우 발생할 수 있는 대량의 오탐지 정보를 추출하고 제거함으로써 탐지의 정확성을 향상시키기는 것을 목적으로 한다. 이러한 방법으로는 분석 데이터의 범위 및 다태성에 따라 동종의 다수 시스템에서 발생하는 이벤트들 간의 연관성을 분석하는 homogeneous log 소스 분석 방법과 이종의 다수 시스템에서 생성되는 이벤트들을 수집하고 정형화하여 연관성을 추출하는 heterogeneous log 소스 분

석 방법이 있다. 이러한 방식은 침입탐지 시스템의 과다 경보를 억제하고 축약하기 위한 경보 연관성 분석 분야 및 침입탐지 시스템의 오탐률을 감소시켜 탐지 성능을 향상시키기 위한 로그 정보 연관성 분석 분야에서 연구되고 있다.

나. 미탐지율 감소

미탐지 관점에서의 미탐지율 보완을 위한 연관성 분석 방법은 알려지지 않은 새로운 공격 패턴을 탐지해내기 위해 통계적이고 확률적인 연관성 분석 방법이 사용된다. 즉, 시그니처 기반의 침입탐지 시스템에서 탐지할 수 없는 새로운 유형의 유해한 행위를 탐지하기 위한 로그 정보 연관성 분석으로 주로 통계적인 수법을 이용하여 시스템 로그의 연관성을 분석하는 분야이다. 이 방법에서는 이상 상태를 추론하기 위하여 정상 상태를 규정하는 baseline 설정을 위하여 Behavior Bayesian 기법, Neural AI 기법과 같은 다양한 수학적 방법들이 이용되며, 연관성 규칙을 생성하기 위한 데이터 마이닝 기법 등도 이용되고 있다. 아직 현실적인 적용 단계에까지는 미치지 못하지만 최근 이 방법에 의한 높은 탐지율이 보고되는 연구 사례가 늘고 있어 향후 주목해야 할 분야이기도 하다.

다. 잠재적 위협의 탐지

Potential threat 관점에서의 잠재적 위협 탐지를 위한 연관성 분석 방법은 아직 진행 단계에 있는 해킹에 의해 잠재적인 위험 요소로 존재하는 침입 흔적을 찾아내기 위해 시간적, 공간적으로 분산되어 있는 로그 정보를 연관 분석하는 분야이다. 포렌식 분야와 유사하지만 포렌식은 발생사건(incident)에 대한 사후 처리를 위하여 어떤 해킹이 이루어진 모든 경위에 대한 완전한 흔적과 이력에 대한 자료를 요구하는 데 반하여 잠재적 위협의 탐지는 특정 공격의 단편적인 흔적을 연관 분석함으로써 attack의 현재 상황을 분석하는 것을 목적으로 한다. Attack에 의해 남겨진 이벤트들의 상태와 그 변화를 관찰하고 각 상태 간의 연관성을 분석함으로써 해킹의 진행 단계를 파악하는 state-based correlation 방법과 특정 attack에 의해 여러 시간축과 공간(로그 소스)축에 남겨진 흔적들 간의 연관성을 분석하여 해킹의 진행 단계를 파악하는 temporal & spatial 방법이 있다[3]. 하지만 이러한 연구들은 아직 상용화 단계에는 못미치고 있으며, 일부 학교 및 연구 기관에 의해서의 학술적인 어프로치로 진행되고 있는 상황이다.

2. 위협 관리 영역

보안이벤트 연관성 분석을 통해 관리 네트워크에 실제 위협이 되는 공격 징후를 선별하고 이들의 심각성을 계산하여 대응에 필요한 우선 순위를 결정하는 위협 관리(threat management) 기능을 제공하는 분야이다. 주로 이종의 보안이벤트간의 연관성을 분석함으로써 단일 정보로는 판단하기 어려운 위협을 발견하는 데 이용된다. 가장 대표적인 방법으로는 IDS 경보와 관리 자산의 취약점을 연관 분석하여 실제 위협을 찾아내는 취약점 연관성 분석이 있다[4].

NIDS와 같이 룰 기반으로 네트워크를 모니터링하여 이상 상태를 감지해 내는 메커니즘은 정의된 룰에 조금만 위배되더라도 이에 대한 경보를 발생시킨다. 따라서 이러한 경보 속에는 실제 관리 네트워크의 위협과는 상관없는 무의미한 정보가 다수 존재할 수 있다. 예를 들면 해킹 툴에 의한 포트 스캐닝을 탐지한 IDS에 의해 발생된 다수의 경보에는 이미 패치되었거나 존재하지 않는 자산에 대한 공격을 탐지한 오경보가 대량으로 포함되어 있을 확률이 크다. 대부분의 해킹 툴은 근원지 주소 또는 목적지 주소를 무작위로 발생시키기 때문이다. 이러한 경보 데이터를 관리 자산의 취약성 정보 및 네트워크 구성 정보와 연관시켜 분석하면 실제 위협에 대한 경보만을 선택적으로 추출할 수 있어 오경보를 대폭 줄일 수 있다. 이와 같이 대량의 오탐지 이벤트 가운데 실제 위협을 선별하고 그 위협들에 대하여 우선순위를 부여한 후 적절한 대응을 수행하는 threat

refining 기술에 보안이벤트 연관성 분석 기술이 이용되고 있다.

비교적 구현이 간단하고 계산 오버헤드가 적기 때문에 앞절의 보안침해 사건 탐지 영역의 연구 결과보다는 광역의 네트워크에 적용할 수 있다. 따라서 network-wide 관점에서의 보안 관리 분야에서 연구 개발이 활발히 진행되고 있으며 많은 상용 제품들에서 채용하고 있는 방법이다. 위협 관리 영역에서 행해지고 있는 주된 연구 동향은 다음과 같다.

가. Vulnerability Correlation

특정 호스트에 대한 IDS의 침입탐지 이벤트와 그 호스트 상의 취약성 정보간의 연관성을 분석하는 방법이다. 해당 공격이 실제로 성공했는가를 추론함으로써 정확한 실제 위협을 추출하고 우선순위에 따라 배열함으로써 빠른 대응을 가능하게 한다. 이를 위해서는 정밀하게 조율된 취약성 스캐너와 그 결과를 수집(import)하는 기능이 필요하다.

나. Watch List Correlation

Watch List와 같이 학습된 입력데이터를 사용하여 이전에 탐지된 공격 정보와 현재의 공격 정보를 연관 분석하여 이전 침입자의 reminder를 제공하는 방법이다.

다. Role-based Correlation

컴퓨터, 컴퓨터 사용자, 경보 등의 동작 및 행위가 주어진 역할 권한에 위배되지 않는가를 연관 분석하여 비정상 행위를 탐지하는 방법이다. 사용 시간에 따라 역할 권한이 변경되는 경우 이러한 세부 정보까지 함께 연관 분석해야 하기 때문에 time correlation이라고도 한다.

라. Open Port Correlation

IDS의 이벤트 등을 통해 현재 호스트상에서 공격당하고 있는 포트 번호와 네트워크 상에서 제공하고 있는 개방된 포트 리스트를 연관 분석하여 해당 공격의 성공 가능성을 결정하는 방법이다. 포트가 개방되어 있지 않은 호스트에 대한 동일 포트 공격과 공격을 필터링함으로써 실제 위협 공격을 가려낸다.

3. 위협 인지 영역

네트워크의 규모와 보안 서비스의 규모가 커짐에 따라 보안이벤트는 기하급수적으로 증가하기 때문에 보안 관리자는 이들 데이터를 분석하여 현재의 네트워크 보안 상황을 즉각적으로 판단하기가 어려워졌다. 위협 인지(threat awareness) 방법은 사용자 인지 관점에서의 분석 방법으로써 관련성있는 이벤트 정보를 하나의 view에 가시적으로 표시함으로써 상호간의 관련성을 사용자가 직관적으로 인지할 수 있도록 하는 방법이다. 즉, 대량의 보안이벤트 정보를 구조화하여 상호간의 관계를 시각화(visualization) 함으로써 관리자가 현재의 보안 상황을 쉽게 인지하도록 하기 위한 연관성 분석 방법이다.

위협 인지 방법으로는 사전에 공격 유형별로 발생하는 각 이벤트 정보간의 연관성을 도출하고 시퀀스를 규정하여 분석한 후 상호간의 상관성을 이해하기 쉬운 형태로 가시화하는 view-based 방식과 다량의 이벤트 정보와 다수의 속성들을 의미있는 정보체로 표현하기 위하여 하나의 view에 다차원적으로 표현하는 event visualization 방법이 있다[5],[6]. View-based 방식은 사전에 분석된 방법을 토대로 시각화를 수행하기 때문에 그려진 결과물에 대한 분석도 어느 정도까지 자동화할 수 있어 대량의 데이터를 처리하는 데 매우 효과적이다. Event visualization은 그려질 대상 이벤트 정보와 속성들을 주기적으로 수집하여 하나의 화면에 축약하여 나타내며 그 결과는 운영자가 판단하도록 하기 때문에 프로세스 부하가 적고 구현이 용이하나 매뉴얼적인 인지를 강조하는 방법이기도 하다. 이처럼 시각화를 이용한 방법들은 분석에 대한 계산 오버헤드가 타 방법에 비하여 비교적 작으며 구현 알고리듬이 단순하여 대량의 데이터를 실시간으로 나타낼 수 있는 장점이 있어 대규모 네트워크의 분석방법으로 유효하다. 하

지만 객관적이고 수치적인 보고기능 처리가 결여되기 때문에 결과에 대한 정확한 판단은 사용자의 직관적인 인지에 의한 의사결정에 맡길 수 밖에 없는 단점이 있다.

4. 포렌식 영역

포렌식(forensics)이란 네트워크상의 모든 원시 데이터 및 타 보안시스템의 로그 데이터를 수집, 과학적인 분석을 통해 네트워크 남용, 내부 자료 도난, 보안 혹은 인력 정책 위반이 기업 자산에 어떤 영향을 미치는지 파악하는 기술이다. 포렌식은 단순 보안 툴간 상호 연관 분석 외에 네트워크 성능 데이터, 트래픽 데이터, 위험 평가 데이터, 지적재산권 보호 정보와 같은 다양한 정보간의 총체적인 연관 분석 기능이 필요하다. 특히 단순 로그 관리가 아닌 당시 공격 상황을 재연하고 설명할 수 있는 법적 증빙 자료로도 사용이 가능한 지식 정보를 생성해야 한다. 따라서 다양한 로그정보 간의 연관성 분석 기술은 이 분야에서는 필수적인 기술이다.

현재까지는 대부분의 포렌식은 전문가의 손에 의한 수작업으로 수행되고 있어 작업 시간, 효율 등에 많은 문제가 있었으나 최근 이러한 작업을 자동화하기 위한 연구가 활발히 이루어지고 있다. 아직 기초적이기는 하지만 profile correlation, route correlation, temporal & spatial correlation 등은 포렌식 기술에 이용될 수 있는 기초적인 방법들이다[3].

5. 보안이벤트 연관성 분석 상용화 제품 동향

최근 많은 보안 장비 벤더 및 네트워크 장비 개발업체에서 보안이벤트 연관성 분석 기술을 제품화한 보안관리 솔루션을 발표하고 있다. 본 절에서는 보안이벤트 연관성 분석 기술의 대표적인 5개의 기능(event reduction, incident detection, threat prioritization, threat awareness, forensics)과 상용 제품들이 제공하는 기능간의 관계를 개략적으로 조사하여 정리하였다. <표 1>에서 속성 1, 2, 3, 4, 5는 각각 event reduction, incident detection, threat prioritization, threat awareness, forensics을 나타내며, ○은 각 사의 제품이 제공하는 기능을, ×는 제공하지 않는 기능을, △는 제공하지만 미흡한 상태를 나타낸다.

〈표 1〉 보안이벤트 연관성 분석 상용 제품 비교

속성	1	2	3	4	5
CheckPoint (Eventia Analyzer)	○	○	○	×	×
Symantec (CyberWolf)	○	○	×	△	×
PRISM (EventTracker)	○	○	×	×	○
GuardedNet (NeuSECURE)	○	○	○	×	×
Intellitactics (ESM)	○	×	○	×	×
ISS (Dynamic Threat Protection)	○	○	○	×	×
NetForensics (nFX)	○	○	○	×	×
Cisco (MARS)	○	○	○	×	×
NetIQ	○	○	×	×	×
OpenService	○	○	×	×	×
Counterpane Internet Security	○	×	○	×	×
GlobalDataGuard (DataGuard)	○	○	×	×	×
Secure Commerce Systems (GuardTower)	○	○	×	×	×

Ⅲ. 시각화기반 보안상황 분석

시각화(visualization)기반 보안상황 분석기술은 네트워크 및 시스템의 대용량, 고속화에 따라 관련 보안 시스템에서 대용량으로 발생하는 보안 이벤트를 실시간 처리하고 그 연관성을 시각적으로 도식화함으로써 알려지지 않은 패턴 분석, 이상상태 표현, 상황예측 등의 보안상황을 관리자가 직관적으로 인지할 수 있도록 하는 기술이다.

1. 기술분야

가. 감시

감시(monitoring)는 현재 발생하고 있는 보안 이

벤트들의 분석을 통해 관리 도메인 상에 이루어지고 있는 보안상황을 지속적으로 지켜보는 것이다. 즉, 가장 최근에 발생한 데이터들을 계속적으로 반영하면서 그것의 상태를 "정상", "준위험", "위험" 등으로 평가할 수 있으며 관리도메인을 세부적으로 뿐만 아니라 전체적으로 표현하여 전체 요약 결과를 한눈에 파악하도록 결과를 계속적으로 제공한다. 또한 다양한 표 또는 그래프를 이용하여 토폴로지 상에 식별력을 갖는 붉은색, 노란색, 녹색 등으로 표현하여 관리자의 보안상황 인지를 도울 수 있다. 보안상황 감시를 하는 데 있어서 중요 이벤트 특성으로는 전체/도메인/호스트별 연결을 맺고 있는 세션 수, 송수신되고 있는 트래픽양, 발생하고 있는 보안 이벤트의 개수 등이 있다[7]. 일례로 이런 감시 활동은 zero day attack과 같이 신속성을 요구하는 분야에 활용도가 높다.

나. 검사

검사(inspecting)는 현재 현상을 유발시킨 원인에 대해 구체적이고 세부적인 데이터들을 찾는 과정이다. 이는 감시와 함께 상황 인지의 식별 단계의 한 부분으로 간주되지만, 특히 검사는 상황 인지의 이해 단계까지 연결된다. 침입탐지는 검사의 좋은 예이다. 일반적으로 시각화를 이용하지 않는 검사는 주어진 데이터집합을 바탕으로 목표에서 벗어난 불필요한 데이터들을 연속적으로 필터링하는 과정이므로 데이터집합에 제약을 받는다. 시각화 기술은 주어진 데이터들을 필터링 이외에 다각도로 표현함으로써 검사 과정을 편리하게 향상시킬 수 있다. 검사 과정을 위한 시각화 특징 요소에는 <표 2>과 같이 연결(세션)의 형태, 연결의 개수, 전송중인 데이터의 양, 연결지속 시간 등이 있다.

다. 탐색

탐색(exploring)은 방향이나 목표가 없이 조사하는 것이다. 이는 사전 지식이나 사전에 정의되지 않은 현상에 대해 시기 적절하게 발견하거나 데이터들의 간의 상호 연관성을 발견하는 것, 그리고 그에 따른 가설이나 이론 등을 생성하는 과정으로 정의할 수 있다. 일반적으로 탐색은 실시간 형태를 취하지는 않는다. 보통 하루 또는 일주일 단위의 데이터를 바탕으로 그리고 단일 시스템/도메인뿐만 아니라 다수의 도메인에 걸쳐 나타나는 현상 또는 비정상적인 모습을 보는 것으로써 최종적으로는 그 현상을 유발시킨 데이터들이 어떻게 그것과 연관되어 있는지 그 특징을 찾는 것이다. 예를 들면, IP-매트릭스 또는 그리드를 이용하여 시간에 따른 전체 트래픽의 패턴이나 보안이벤트의 동향을 보는 것은 탐색의 좋은 예이다. 이와 같이 시각화는 알려지지 않은 트래픽 패턴 및 동향, 이상 현상을 인지할 수 있는 "visual discovery"라고 말할 수 있다[7].

라. 예측

예측(forecasting)은 과거의 현상이나 패턴들을 토대로 현재 진행되고 있는 일련의 행동들을 파악하여 다음 단계의 결과를 사전에 인지하는 것으로써 관리자들로 하여금 대응 행동을 결정하는 데 도움을 준다. 예측을 수행하기 위해서는 현재의 세부 데이터 및 현재의 시스템 지식뿐만 아니라 과거에 발생

〈표 2〉 검사에 이용되는 특징 요소

특징 요소	표현 방법	현상 예
다대일 연결 형태	노드들 간의 연결을 표현	Denial of Service Attack
일대다 연결 형태	노드들 간의 연결을 표현	Scanning, Worm
연결의 개수	네트워크(노드들)의 연결 상황을 표현	Worm
전송중인 데이터의 양	선택된 노드들에 대해 전송 데이터양을 표현(선의 굵기)	이상 현상, 트래픽 동향
연결 길이	연결 지속 시간을 표현	이상 현상, 트래픽 동향

했던 유사한 패턴이나 데이터가 반드시 필요하다[7]. 따라서 예측을 수행하기 위한 시각화 기술은 상황 재연이나 패턴/동향 기반 탐색(pattern-based searching)을 지원함으로써 관리자가 공격자의 다음 행동들을 신속히 파악하고 관리 도메인을 방어할 수 있는 적절한 결정을 내리도록 도울 수 있다.

마. 전달

데이터의 시각화 결과는 해당 현상을 전달(보고, communicating)하는 데 유용하게 이용될 수 있으며, 동일 분야의 관심 있는 다른 사람들과의 의사소통을 편리하게 만드는 도구로 사용될 수도 있다. 또한, 그 결과는 동일 분야의 일을 수행하는 사람들을 교육시키거나 대응했던 행동들에 대해 검토 및 평가를 수행하는 데에도 유용하게 이용될 수 있다[7]. 이는 다른 전문가들에 의해 그리고 인터넷의 활성화된 토론(협회)들로부터 보다 나은 대응 결정을 이끌어내어 유용하게 사용될 수 있다.

2. 기술분류

네트워크의 보안상황 인지를 위한 이벤트 시각화 기술 및 도구들은 그 목표가 호스트의 상황이냐 네트워크의 상황이냐에 따라 크게 두 가지로 나눌 수 있다. 대부분의 호스트 상황은 프로세서(CPU), 메모리, 응용 프로세스, 네트워크 포트 등의 감시를 통해 이루어지며, 네트워크 상황은 개별 호스트, 서브네트워크, 전체 네트워크, 연결 상황, 프로토콜, 포트 등을 종합적으로 감시하여 표현한다.

가. 호스트 뷰(view) 도구

기본적인 프로세스나 네트워크 소켓(socket)을 감시하는 도구들(Unix 부류의 운영체제에서 제공하는 netstat, top 명령어)들을 이용하거나 기타 프로세스 감시 도구들을 이용하여 호스트들의 보안상황을 표현하는 도구들이 이 부류에 속한다. 대표적인 예로는 NCSA의 Clumon[8], 버클리대학(UC. Berkeley)의 Ganglia[9], 스탠포드(Stanford) 대학의 Rivet[9], SIFT의 NVisionCC[10]가 있으며, 특히 NVisionCC는 클러스트 환경의 호스트들까지 보안상황을 표현할 수 있는 기능이 있다.

나. 네트워크 뷰 도구

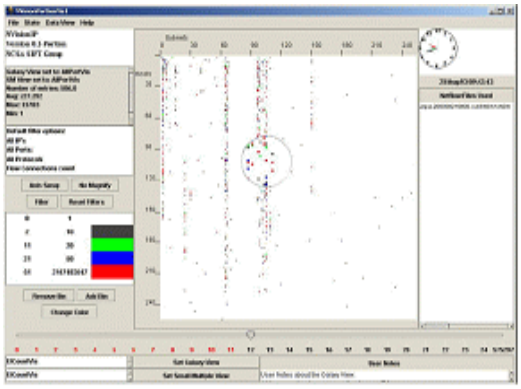
대부분의 네트워크 보안상황 시각화 기술은 여기에 속한다. 가장 간단하게는 패킷의 헤더 정보(송신지 주소, 목적지 주소, 프로토콜, 포트 번호)를 이용하여 2/3차원 공간에 표현하는 것에서부터 IDS, FW 등의 이벤트 내용을 표현하는 것이 있다. 패킷의 헤더 정보를 이용하는 대표적인 예로는 NVisionIP[11], VisFlowConnect[12], 그리고 PortVis[13]가 있으며 이런 도구들은 호스트 기반의 데이터들과 연동을 하지 않는 특징이 있다. 반면에, IDS나 FW 이벤트를 시각화하는 도구들은 호스트 기반의 이벤트들과 연동을 하기도 하며 여러 위치의 센서, 수행 능력, 중요도 등에 따라 이벤트들을 재배치하고 연관 관계를 그래픽하게 표현한다. 대표적인 예로는 Potential Doom사의 Spinning Cube[14], Secure Decision사의 SecureScope[15] 등이 있다.

3. 기술동향

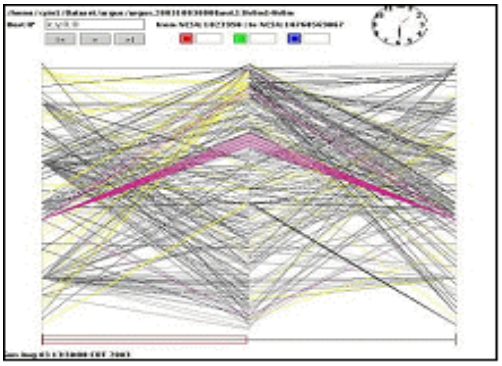
가. NVisionIP[11], VisFlowConnect[12]

NCASSR의 SIFT는 보안상황 인지를 위한 대표적인 도구들로써 Cisco의 Netflow 데이터를 이용한다.

NVisionIP는 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 view, machine view 등의 drill-down 기능을 제공한다((그림 2) 참조). VisFlowConnect는 보안상황 인지를 위해 세션(연결)



(그림 2) NVisionIP

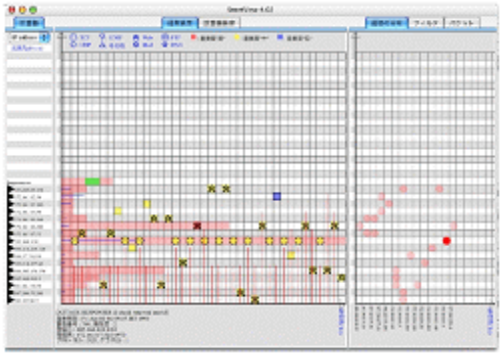


(그림 3) VisFlowConnect

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 트래픽양을 표현하고 있으며 연결선의 색은 사전에 정의된 도메인을 의미한다((그림 3) 참조).

나. SnortView[16]

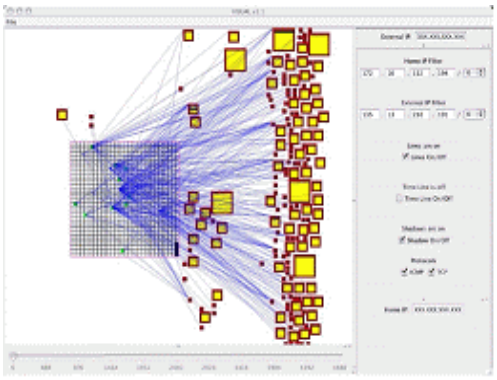
NIDS인 snort의 로그를 이용하여 매트릭스 형태로 표현, 근원지/목적지 IP 주소와 프로토콜 정보를 바탕으로 이벤트 종류 및 우선순위에 따라 해당 이벤트의 아이콘과 중요도(색깔)를 표시한다. 이벤트의 개수는 막대그래프의 높이를 통해 알 수 있으며 해당 연결을 선택할 경우 근원지-목적지 간의 상세 정보를 화면 하단에 표시한다((그림 4) 참조).



(그림 4) SnortView

다. Visual[17]

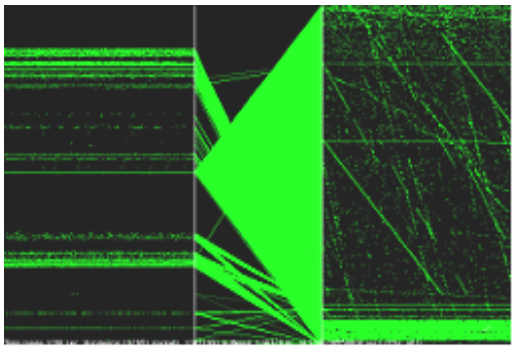
입력 데이터로 PCAP 파일을 가공한 패킷 추적(trace) 정보를 이용한다. 일반적으로 공격자가 시도하는 포트 스캐닝, 핑(ping) 스캐닝 등을 쉽게 검출할 수 있으며 네트워크의 통신 패턴을 인지하기에 좋은 도구이다. 1000개 보다 작은 호스트들로 구성되는 서브-네트워크의 포렌식 분석에 이용되며 비정상적인 현상을 감시하기에는 적절하지 않다. 세분화 기능을 위한 fan-in, fan-out 기능이 제공되며 시스템 로그나 IDS 로그는 사용하지는 않는다((그림 5) 참조).



(그림 5) Visual

라. Visual Fingerprinting[18]

네트워크 트래픽과 보안상황을 감시하기 위한 도구로써 네트워크/호스트들의 트래픽 패턴을 실시

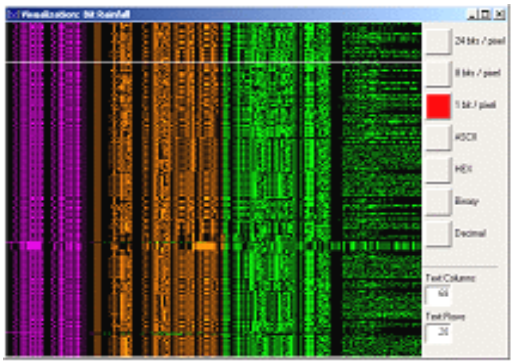


(그림 6) Visual Fingerprinting

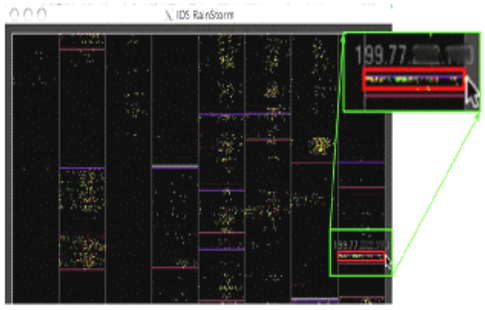
간으로 표현하며 포렌식을 위한 상황 재연(play-back) 기능을 포함하고 있다. 일반적으로 네트워크 공격 도구들의 특징과 공격 이후에 나타나는 호스트들의 현상들을 표현한다. 이 도구는 웜(worm)과 분산서비스거부(DDoS) 공격을 감시하기에 좋은 도구이다((그림 6) 참조).

마. RainFall[19] 및 RainStorm[20]

RainFall은 2진수(bit)로 표현되는 트래픽의 헤더와 내용을 픽셀에 매치시켜 시각화함으로써 특정 근원지, 목적지, 프로토콜, 포트 등의 패턴을 찾는다((그림 7) 참조). 반면에, RainStorm은 IDS 이벤트를 이용하여 근원지/목적지 주소를 Y축, 시간을 X축으로 설정하고 네트워크의 상황을 표현한다((그림 8) 참조). 이들은 현재 알려지지 않은 새로운 공격이나 패턴을 생성하는 데 이용될 수 있다.



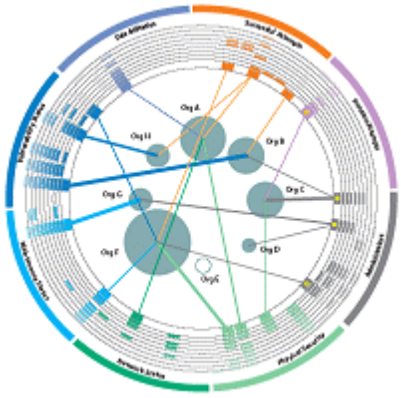
(그림 7) RainFall



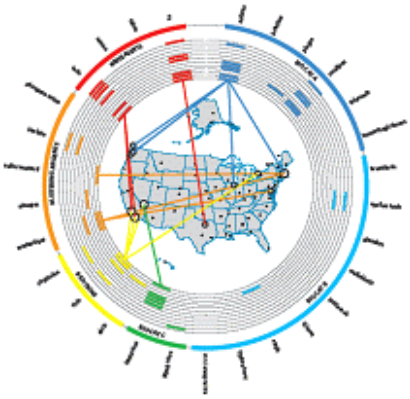
(그림 8) RainStorm

바. VizAlert, VisAware[21]

Utah 대학에서 개발한 도구로써 IDS 이벤트들의 특징(w3 premise: what, when, where)을 기반으로 시각화하여 전체/개별 관리 도메인의 보안 상황을 인지하도록 한다. VizAlert은 관리 도메인을 중심부에 두고 시간 주기를 의미하는 원들을 중심에서 외부로 그려서 표현하고 있으며, 가장 외부에는 연관성 있는 이벤트의 그룹들을 표현하고 있다((그림 9) 참조). VizAware는 관리 도메인을 토폴로지 정보와 결부시켜 표현하고 있으며 이벤트를 생성한 센서들의 정보를 가장 외부 원상에 표현하여 해당 이벤트의 상세 정보를 제공한다((그림 10) 참조)). VizAlert과 VisAware는 네트워크 보안상황 인지 이외에 범용적으로 911, 소방서, 경찰서 등과 긴급구호 센터, 그리고 질병관리국의 BioWatch 등에 활용될 수 있다.



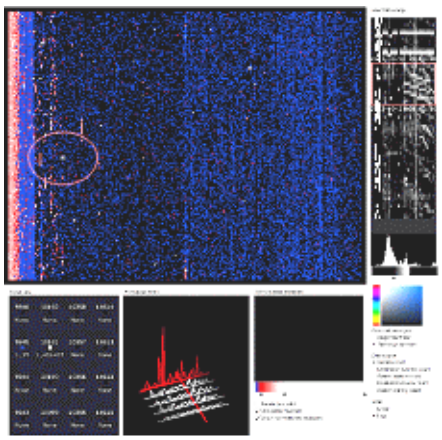
(그림 9) VizAlert



(그림 10) VizAware

사. PortVis[13]

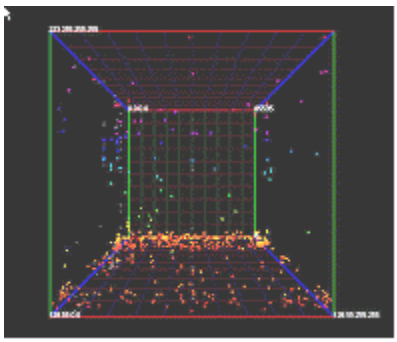
UC. Davis에서 개발한 도구로써 포트 기반의 네트워크 보안상황 인지 도구이다. 대규모 네트워크 환경에 적용할 수 있으며, 동일 정보를 여러 각도로 표현하여 관리자로 하여금 데이터간의 상호 연관성을 인지시킬 수 있다. 관리자는 표현 기간을 임의로 설정하여 네트워크를 감시할 수 있으며 비정상적인 현상들을 검출하기에 매우 좋은 도구이다. 기본적인 drill-down 기능은 있지만, 해당 현상에 대한 상세 데이터를 표현하는 것은 제한적이다((그림 11) 참조).



(그림 11) PortVis

아. The Spinning Cube of Potential Doom[14]

NERSC에서 개발한 보안상황 인지 도구이다.

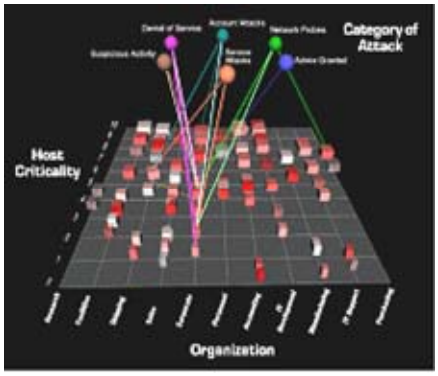


(그림 12) Spinning Cube

3차원 공간을 구성하는 X축은 내부 IP 주소 범위, Z축은 전체 IP 주소 범위, Y축은 포트 범위를 의미한다. 주로 스캐닝 공격을 검출하는 데 유용하며, 포트 스캐닝 공격일 경우 세로로 연속된 선이 나타나고 네트워크(호스트) 스캐닝 공격은 가로 형태의 선이 나타난다((그림 12) 참조).

자. SecureScope[15]

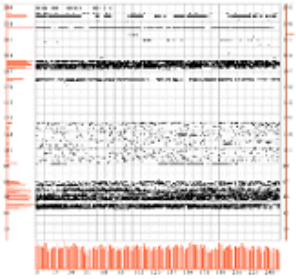
Secure Decision에서 개발한 도구로써 IDS, Scanner, FW에서 발생하는 이벤트를 시각화한다. 관리 네트워크(도메인) 내의 자원과 이벤트를 함께 표현하여 현재의 보안상황 정보를 보여주며, 패턴 검색 및 동향에 대한 정보도 제공한다. 특히, 이 도구는 이벤트의 종류와 심각도 이외에 이벤트들 간의 연관성을 결합하여 공격의 유형 및 이상 행동까지 보여줄 수 있으며, 세부적인 호스트와 운영체제에 따른 보안상황 정보도 제공한다((그림 13) 참조).



(그림 13) SecureScope

차. IP Matrix[22]

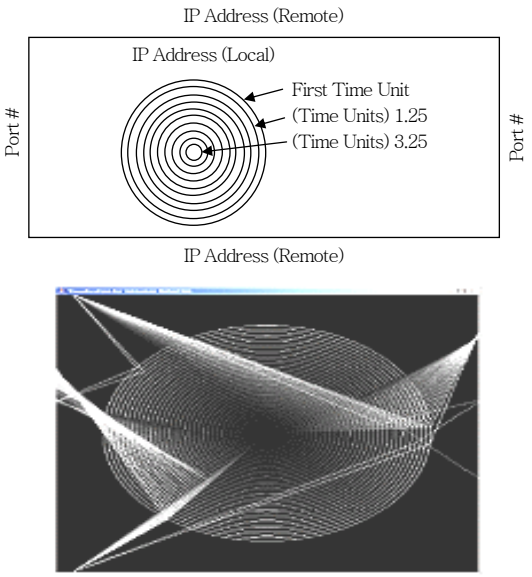
일본 전기통신대학에서 개발한 시각화 도구이며 class B 주소 체계를 갖는 도메인의 전체 네트워크 및 내부 네트워크의 보안 현황을 감시할 수 있다. 로그 서버의 이벤트(snort alert)로부터 수집하여 IP matrix 상에 표현함으로써 공격 및 공격 유형을 판단할 수 있다. 이 도구는 특정 시간대(구간)의 스냅-샷만을 제공한다((그림 14) 참조).



(그림 14) IP Matrix

카. IDS Challenges[23]

Utah State 대학에서 개발한 이 도구의 정확한 명칭은 아직 없다. IDS 이벤트를 수집하여 (그림 15)에서 보는 바와 같이, 공격자(dst, port)와 피해자(src, port)를 모두 표시함으로써 네트워크의 보안 상황을 표현한다. 그리고 시간은 원형축을 확장하여 공격의 진행 절차가 표시될 수 있도록 했다.



(그림 15) IDS Challenges

Ⅳ. 결론

네트워크 차원에서 보안 침해 요인을 분석하고 이에 대한 대응 방안을 적용하고자 하는 노력은 최근에서야 시작되었다.

이를 위해서는 기존의 보안 시스템으로부터 발생하는 다량의 보안 경보 이벤트에 대한 분석을 통해 현재 관리 대상 도메인 네트워크의 보안상황에 대한 실시간에 가깝고 오탐이 없는 정확한 분석이 필요하다. 만약 분석이 신속하게 이루어지지 않을 경우 공격 및 그 피해의 전파속도, 범위가 신속하고 광역화되는 현재의 추세를 감안할 때 공격 발생 상황에 대한 대응이 늦어져 네트워크 전체로의 마비로 이어질 수 있다. 정확하지 않은 분석을 토대로 대응이 이루어질 경우 네트워크 내 정당한 사용자나 그 사용자의 트래픽을 제어하여 서비스 이용을 방해하는 역효과를 가져오게 된다. 이런 중요성과 네트워크 및 시스템의 대용량화, 고속화로 인한 발생 이벤트의 대량화 때문에 단순 보안 상태 정보가 아니라 보안상황 인지가 가능한 지식을 제공하기 위한 보안이벤트의 연관성 분석과 그 일환으로 보안 이벤트를 시각화하고 분석하여 그래프로 제공함으로써 사용자가 직관적으로 보안상황을 인지할 수 있는 기술에 대한 개발이 활발히 진행되어 시각화기반의 경우 상당한 발전을 이룬 상태이다.

공격 및 그 피해의 신속성을 감안할 때 보안이벤트 연관성 분석의 결과로써 그 이상 유무를 자동적으로 판단해 이를 대응까지 일관적으로 시스템화할 필요성은 점점 증가하고 있으나 시각화에 기반한 보안상황 분석의 경우 그 판단을 사용자가 수행함으로써 대응까지 시스템화하여 자동적으로 수행하기에는 어려운 단점이 있다. 또한 시각화를 제외한 타 보안이벤트 연관성 분석 분야의 경우 자동화할 수 있는 분석 결과는 제공하나 아직 그 분석 결과의 신뢰

성에 대한 검증이 확실이 이루어지지 않아 이에 대한 연구가 추가적으로 필요하다고 볼 수 있다.

약 어 정 리

DDoS	Distributed Denial of Service
FW	Firewall
IDS	Intrusion Detection System
NCASSR	National Center for Advanced Secure Systems Research
NERSC	National Energy Research Scientific Computing Center
NIDS	Network IDS
PCAP	Packet CAPture
SIFT	Security Incident Fusion Tool

참 고 문 헌

[1] Cristina Abad, Jed Taylor, Cigdem Sengul, and Yuanyuan Zhou, "Log Correlation for Intrusion Detection: A Proof of Concept," *19th Annual Computer Security Applications Conf.*, Dec. 8-12, 2003.

[2] Xiaoxin Yin, Kiran Lak karaju, Yifan Li, and William Yurcik, "Selecting Log Data Sources to Correlate Attack Traces for Computer Network Security: Preliminary Results," *Int'l Conf. on Telecommunications Modeling and Analysis*, 2003.

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

[4] Cynthia Phillips and Laura Painton Swiler, "A Graph-Based System for Network-Vulnerability Analysis," http://citeseer.ist.psu.edu/356646.html

[5] Cristina Abad, Yifan Li, and Kiran Lakkaraju, "Correlation between NetFlow System and Network Views for Intrusion Detection," http://www.projects.ncassr.org/sift/papers/icdm04.pdf

[6] Herv Debar and Andreas Wespi, "Aggregation and Correlation of Intrusion-Detection Alerts," http://perso.rd.francetelecom.fr/debar/papers/DebWes01.pdf

[7] A. D'Amico and M. Kocka, "Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned," *IEEE Symp. on Information Visualization's Workshop on Visualization for Computer Security (VizSEC)*, Oct. 2005.

[8] T. Roney, A. Bailey, and J. Fullop, "Cluster Monitoring at NCS," *2nd LCI Int'l Conf. on Linux Clusters*, 2001.

[9] M. Massie, B. Chun, and D. Culler, "The Ganglia Distributed Monitoring System: Design, Implementation, and Experience," *Parallel Computing*, Vol.30, Issue.7, 2004.

[10] W. Yurcik, X. Meng, and N. Kiyanclar, "NVisionCC: a Visualization Framework for High Performance Cluster Security," *Proc. of VizSEC 2004*, ACM Press, New York, NY, USA, Oct. 2004, pp.133-137.

[11] K. Lakkaraju, W. Yurcik, and A. Lee, "NVisionIP: Netflow Visualizations of System State for Security Situational Awareness," *Proc. of VizSEC 2004*, ACM Press, New York, NY, USA, Oct. 2004, pp.65-72.

[12] X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju, "VisFlowConnect: Netflow Visualizations of Link Relationships for Security Situational Awareness," *Proc. of VizSEC 2004*, ACM Press, New York, NY, USA, Oct. 2004, pp.26-34.

[13] J. McPherson, K. Ma, P. Krystosek, T. Bartoletti, and M. Christensen, "PortVis: A Tool for Port-Based Detection of Security Events," *Proc. of VizSEC 2004*, ACM Press, New York, NY, USA, Oct. 2004, pp.73-81.

[14] Stephen Lau, "The Spinning Cube of Potential Doom," *Commun. of the ACM*, Vol.47, No.6, ACM Press, New York, NY, USA, Oct. 2004, pp.25-26.

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

[16] H. Koike and K. Ohno, "Snortview: Visualization System of Snort Logs," *In ACM*, editor, VizSEC/DMSEC'04, Washington DC, USA, Oct. 2004.

[17] R. Ball, G. Fink, and C. North, "Home-centric Visualization of Network Traffic for Security Administration," *ACM Conf. on Computer and Commun. Security's Workshop on Visualization and Data Mining for Computer Security (VizSEC)*, Oct. 2004, pp.55-64.

[18] G. Conti and K. Abdullah, "Passive Visual Fingerprinting of Network Attack Tools," *ACM Conf. on Computer and Commun. Security's Workshop on*

Visualization and Data Mining for Computer Security (VizSEC), Oct. 2004.

[19] G. Conti, J. Grizzard, M. Ahamad, and H. Owen, "Visual Exploration of Malicious Network Objects Using Semantic Zoom, Interactive Encoding and Dynamic Queries," *IEEE Symp. on Information Visualization's Workshop on Visualization for Computer Security (VizSEC)*, Oct. 2005.

[20] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko, "IDS RainStorm: Visualizing IDS Alarms," *IEEE Symp. on Information Visualization's Workshop on Visualization for Computer Security (VizSEC)*, Oct. 2005.

[21] Y. Livnat, J. Agutter, S. Moon, and S. Foresti, "Visual Correlation for Situational Awareness," *Proc. of IEEE 2000 Symp. on Information Visualization (InfoVis)*, Oct. 2005.

[22] H. Koike, K. Ohno, and K. Koizumi, "Visualizing Cyber Attacks Using IP Matrix," *IEEE Symp. on Information Visualization's Workshop on Visualization for Computer Security (VizSEC)*, Oct. 2005.

[23] R. Erbacher, K. Christensen, and A. Sundberg, "Designing Visualization Capabilities for IDS Challenges," *IEEE Symp. on Information Visualization's Workshop on Visualization for Computer Security (VizSEC)*, Oct. 2005.