네트워크 보안 이벤트 시각화 기술

Visualization Technology of Network Security Events

21세기를 대비하는 정보보호 특집

정치윤 (C.Y. Jeong) 보안관제기술연구팀 연구원
장범환 (B.H. Chang) 보안관제기술연구팀 선임연구원
나중찬 (J.C. Na) 보안관제기술연구팀 팀장

목 차

최근 이루어지는 사이버 공격들의 형태가 점점 더 다양해지고 공격의 전파 속도가 빨라짐에 따라 기존의 침임 탐지 기법으로는 이러한 공격을 신속하게 탐지하고 차단하기에는 한계가 있다. 이와 같은 문제점을 해결하기 위해서 최근에 네트워크 보안 이벤트 시각화 기술에 대한 연구가 활발히 진행되고 있다. 네트워크 보안 이벤트 시각화 기술은 네트워크 상에서 발생되는 방대한 양의 이벤트를 실시간으로 시각화함으로써 네트워크 공격의 탐지, 알려지지 않은 공격 패턴 분류, 네트워크 이상 상태의 발견 등 네트워크 보안 상황을 관리자가 직관적으로 인지할 수 있도록 하는 기술이다. 본 고에서는 보안 이벤트 시각화 기술을 유선 네트워크와 무선 네트워크로 구분하여, 각각의 네트워크 환경에서 현재 개발되고 있는 기술의 동향과 앞으로의 발전 방향에 대해서 다루도록 한다.

I. 서론

최근 서비스 거부 공격, 분산 서비스 거부 공격 등의 사이버 공격이 사회적 이슈로 부각하면서 기존의 침입탐지시스템의 한계점이 드러나고 있다. 침입탐지시스템의 경우 공격에 대한 시그니처를 기반으로 하는 오용탐지기법(misuse detection)과 정상적인 네트워크의 상황을 분석하여 네트워크 상태 모델을 생성한 후 비정상 행위를 탐지하는 비정상 행위 기반 탐지기법(anomaly detection)이 있다. 시그니처 기반의 오용탐지 기법을 사용하는 침입탐지시스템의 경우 약 1500~2000개의 네트워크 공격에 대한 시그니처를 탑재할 수 있으나, 1년에 1000개 이상의 새로운 위협들이 발생하기 때문에 새로운 시그니처를 탑재하기 위해서는 기존의 시그니처를 삭제해야 한다[1]. 따라서 이전에 발생했던 위협이 다시 발생하는 경우에는 공격에 그대로 노출될 수 있다. 또한 새로운 공격에 대한 시그니처를 생성하는 데 2~4일이 소요되기 때문에 제로데이(zero-day) 위협에 대처할 수 없는 문제점이 있다. 비정상 행위기반 탐지기법의 경우에는 정상적인 상태의 네트워크를 분석하여 정상 행위에 대한 모델을 생성해야 하는데, 정상 행위에 대한 정의가 사람마다, 네트워크마다 다를 수 있기 때문에 정상 행위에 대한 모델을 생성하는 데 어려움이 있다. 또한 오탐율(false positives)이 높기 때문에 아직 비정상 행위기반 탐지기법이 많이 사용되지 않고 있다.

이와 같은 침입탐지시스템의 문제점을 해결하고 네트워크 공격에 효과적으로 대처하기 위해서 최근에는 네트워크 보안 이벤트 시각화 기술에 대한 연구가 활발히 진행되고 있다. 네트워크 보안 이벤트 시각화 기술은 네트워크상에서 발생되는 방대한 양의 이벤트를 실시간으로 시각화함으로써 네트워크 공격의 탐지, 알려지지 않은 공격 패턴 분석, 네트워크 이상 상태의 발견 등 네트워크의 보안 상황을 관리자가 직관적으로 인지할 수 있도록 하는 기술이다. 사람의 시력은 초당 150Mbyte 정보를 스크린 상에서 처리가 가능하며, 고도의 대조적인 시각효과(색상, 움직임, 모양 등)도 충분히 식별할 수 있다고 알려져 있다. 따라서 네트워크 보안 이벤트 시각화 기술을 사용하면 보안과 관련된 많은 정보를 네트워크 관리자에게 신속하고 쉽고 정확하게 전달할 수 있다. 또한 네트워크 상에서 발생하는 모든 이벤트를 정보의 축약없이 화면상에 표현하기 때문에 알려지지 않은 공격, 제로데이 위협에 대해서도 관리자가 인지할 수 있다는 장점이 있다.

따라서 본 고에서는 현재 개발되고 있는 네트워크 보안 이벤트 시각화 기술을 유선 네트워크와 무선 네트워크로 구분하여 다루고자 한다.

Ⅱ. 유선 네트워크에서의 시각화 기술

유선 네트워크에서의 시각화 기술은 보안 이벤트를 네트워크의 어떤 지점에서 전송하는지에 따라서 목적이 달라지게 된다. 보안 이벤트를 전송하는 지점은 호스트 내부, 네트워크에 연결된 호스트, 네트워크 장비 등으로 구분될 수 있으며, 본 고에서는 네트워크 장비로부터 보안 이벤트를 수신하여 네트워크의 보안 상황을 시각화하는 기술만으로 한정하여 다룰 것이다.

유선 네트워크에서의 보안 이벤트 시각화 기술이 사용할 수 있는 보안 이벤트는 크게 트래픽 이벤트와 경보 이벤트로 구분될 수 있으며, <표 1>과 같은 정보들이 보안 이벤트 시각화를 위하여 사용될 수 있다. 트래픽 정보의 경우 핵심 5-tuples 정보(트래픽의 목적지, 근원지, 목적지 포트, 근원지 포트, 프로토콜) 이외에도 다른 부가적인 많은 정보들을 가지고 있는 반면에, 경보 이벤트는 핵심 5-tuples의 정보를 모두 가지고 있는 경우가 드물다. 대신 탐지

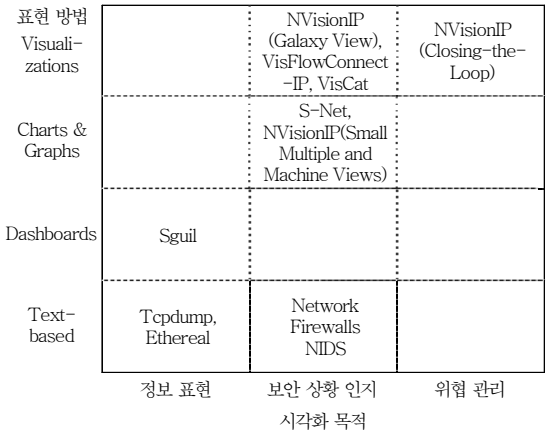
〈표 1〉 유선 네트워크에서의 보안 이벤트

트래픽 정보	- CISCO NetFlows(v1/3/5/7/9) - cFlows - sFlows - IPFIX
경보 데이터	- Intrusion Prevention System - Intrusion Detection System - Firewall/WebFireWall

된 공격의 이름, 적용된 룰 정보 등의 부가적인 정보들을 가지고 있다. 현재 유선 네트워크에서의 보안 이벤트 시각화 기술은 주로 트래픽 정보를 사용하여 개발되고 있으며, 그 중 CISCO사의 Netflow 정보를 사용하는 경우가 많다.

본 고에서는 유선 네트워크에서의 보안 이벤트 시각화 기술을 (그림 1)과 같이 분류하였다. 유선 네트워크의 시각화 기술은 보안 이벤트를 표현하는 방법과 시각화의 목적에 따라서 구분될 수 있으며, 보안 이벤트를 표현하는 방법에 따라서 텍스트, 대시보드, 차트와 그래프, 시각화 방법으로 구분될 수 있다[2]. 시각화의 목적은 보안 이벤트 및 보안 이벤트의 축약 정보를 단순히 표현하는 정보 표현 단계, 보안 이벤트의 상세 정보를 표현함으로써 현재 네트워크의 보안 상황을 직관적으로 인지할 수 있도록 하는 보안 상황 인지 단계, 보안 이벤트의 상세 정보 표현 및 관리자의 개입으로 대응하는 정책을 생성할 수 있는 위협 관리 단계로 구분될 수 있다.

초기에 개발된 텍스트를 기반으로 보안 이벤트를 표현하는 방법들은 네트워크 관리자에게 네트워크에 관련된 정보를 전달하는 것을 주된 목적으로 하고 있었으며, 대표적인 방법으로는 Tcpdump, Ethereal 등이 있다. 현재 유선 네트워크에서의 시각화 기술은 보안 상황인지를 위한 기술들이 주로 개발되고 있으며 대표적인 방법으로는 NVisionIP[3], VisFlowConnect-IP[4], VisCat 등이 있다. 보안 상황인지를 목적으로 하는 시각화 기술의 경우 탐지된 공격에 대한 대응을 수행하기 위해서는 별도의 기술이나 절차를 필요로 하는 것이 단점으로 지적되었다. 그래서 최근에는 네트워크 보안 이벤트 시각화 기술을 사용하여 네트워크의 보안 상황을 인지한 후 공격에 대응하기 위한 위협 관리를 목적으로 하는 기술들이 개발되고 있다.



(그림 1) 유선 네트워크 시각화 기술 분류

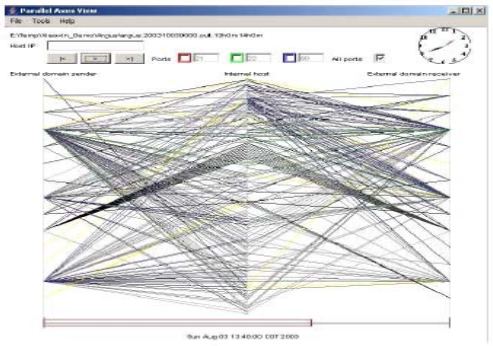
본 고에서는 보안 상황인지를 위한 대표적인 VisFlowConnect-IP, VisCat 방법과 위협관리를 목적으로 하는 NVisionIP(Closing-the-Loop)[5]에 대해서 살펴볼 것이다.

1. VisFlowConnet-IP

VisFlowConnect-IP는 X. Yin et al.[4]에 의해서 2004년에 제안된 방법으로 Netflow 데이터를 사용하여 보안 상황인지를 목적으로 개발되었으며, 보안 이벤트의 표현 방법으로 시각화를 사용한다. VisFlowConnect-IP는 평행 축(parallel axis)을 이용한 External View, Domain View, Internal View의 세 화면과 Host Statistics View로 구성된다. 평행 축에서 각 선들을 구성하는 한 점은 호스트, 네트워크, 또는 특정 도메인을 나타내며, 평행 축을 이용한 시각화 방법은 네트워크에서 발생하는 트래픽을 평행 축을 구성하는 점과 점을 선으로 연결하는 방법이다.

가. External View

External View는 내부 도메인과 외부의 인터넷 도메인간의 연결 정보를 보여주는 화면으로 세 개의 가로 축으로 구성되어 있으며, 각 축은 데이터를 송신하는 외부 도메인, 내부 도메인 내의 호스트, 데이터를 수신하는 외부 도메인으로 구성되며 (그림 2)와 같다. 각 축을 연결하는 연결선은 트래픽을 의미하며, 사전에 정의된 임계치를 초과하는 트래픽에 대해서만 연결선을 표시하게 된다. 트래픽의 양이 많아질수록 연결선이 어두운 색을 띠며, 선의 굵기

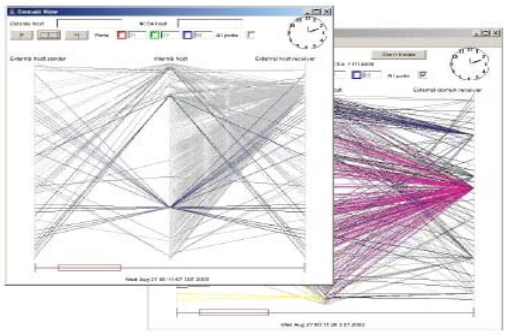


(그림 2) External View[4]

가 굵어지게 된다. 연결선의 색은 사전에 정의된 도메인을 의미한다.

나. Domain View

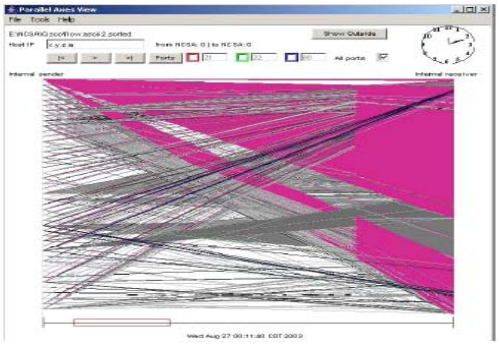
Domain View는 전체 외부 도메인 중 선택된 도메인과 내부 도메인간의 연결 정보를 보여주는 화면으로 (그림 3)과 같다. Domain View를 구성하는 세 축은 선택된 트래픽을 송신하는 외부 도메인, 내부 도메인의 호스트, 데이터를 수신하는 외부 도메인으로 구성된다. 이때 외부 도메인은 사용자에 의해서 선택된 외부 도메인을 의미한다. 선택된 외부 도메인에 대한 연결 정보만을 화면상에 보여주기 때문에 네트워크 관리자는 좀 더 직관적으로 트래픽의 흐름을 파악할 수 있게 된다. 또한 애니메이션을 통하여 시간의 흐름에 따른 트래픽의 변화, 특정 시간에서의 트래픽 흐름 등을 볼 수 있게 됨으로써 이상 현상을 판단하는 데 도움을 줄 수 있다.



(그림 3) Domain View[4]

다. Internal View

Internal View는 내부 도메인의 호스트간에서 발생되는 연결정보를 보여주는 화면으로 (그림 4)와 같다. Internal View의 왼쪽 축은 데이터를 보내는 내부 호스트, 오른쪽 축은 데이터를 수신하는 내부 호스트를 의미한다. Internal View는 내부 네트워크를 대상으로 하는 공격을 인지하는 데 유용하게 사용될 수 있다.

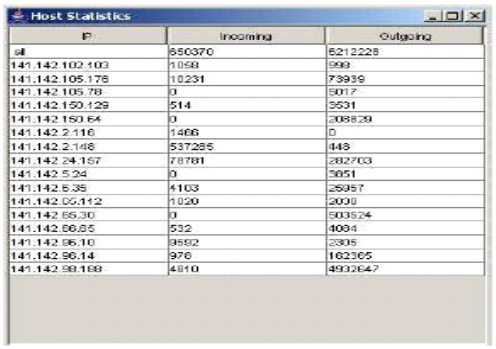


(그림 4) Internal View[4]

라. Host Statistics View

Host Statistics View는 사용자의 요구가 있을 때, 사용자가 선택한 호스트와 연결되었던 호스트들의 누적된 트래픽에 대한 통계 정보를 제공하며, (그림 5)와 같다.

VisFlowConnect-IP의 경우 네 개의 화면을 사용하여 드릴다운(drill-down) 기능을 제공하며 전체 네트워크 관점에서의 네트워크의 상황뿐만 아니



(그림 5) Host Statistics View[4]

라 호스트에 대한 상세한 통계 정보까지 제공해 줄 수 있다. 또한 VisFlowConnect-IP를 사용하면 네트워크 공격에 대한 패턴을 쉽게 인지할 수 있기 때문에 네트워크 관리자가 현재 보안 상황을 이해하는 데 있어 도움이 된다. 하지만 몇 개의 선택된 포트 번호에 해당하는 트래픽만 화면상에 표현할 수 있으며, 임계값을 넘지 않는 트래픽의 경우 화면상에 표현되지 못한다. 또한 네트워크 관리자가 상세한 정보를 얻기 위해서 화면을 계속 전환해야 하므로 이상현상을 파악하는 데 있어서 시간이 많이 소요되는 단점이 있다.

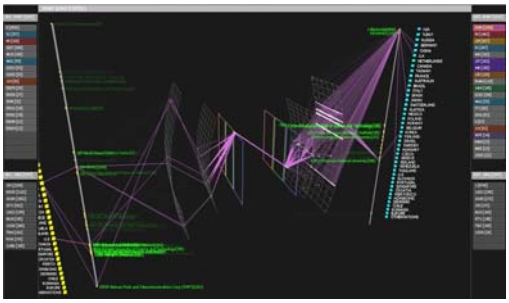
2. VisCat

VisCat(Visualization of Cyber Attacks)은 ETRI에서 2007년에 개발한 네트워크 보안 이벤트 시각화 기술이다. VisCat은 보안 상황인지를 목적으로 개발되었으며, 보안 이벤트의 표현 방법으로 시각화를 사용하며 트래픽과 경보 이벤트를 한 화면에 표시할 수 있다. VisCat은 VisCat/IPGrid, VisCat/Center, VisCat/Globe 등의 세 가지 화면으로 구성되어 있으며, 다음과 같은 정보들을 한 화면에 표현할 수 있다.

- <근원지 IP, 근원지 포트, 프로토콜, 목적지 포트, 목적지 IP>로 구성된 연결 정보
- 근원지 IP와 목적지 IP의 국가 및 ISP
- 근원지 IP와 목적지 IP의 물리적 위치

가. VisCat/IPGrid

VisCat/IPGrid는 IP 주소를 표현하는 IPGrid를 사용하여 전체 IP 주소공간에서 발생하는 연결 정보를 표현하며, (그림 6)과 같다. VisCat/IPGrid는 전체 IP 공간을 표현하기 때문에 호스트 스캔, 포트 스캔과 같은 각종 스캐닝 공격을 식별력 있게 표현할 수 있다. 또한 특정 B클래스 네트워크, 특정 근원지 및 목적지 포트, 특정 국가 및 ISP를 선택하여 네트워크 관리자가 원하는 이벤트만을 필터링하여 볼 수

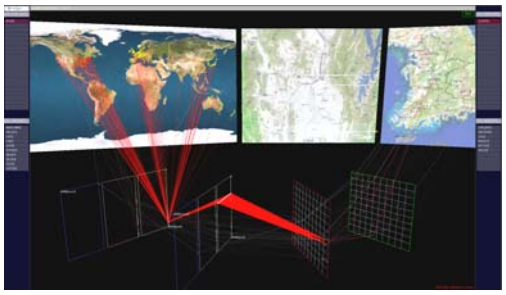


(그림 6) VisCat/IPGrid

있기 때문에 네트워크의 이상현상을 직관적으로 파악하는 데 도움이 된다.

나. VisCat/Center

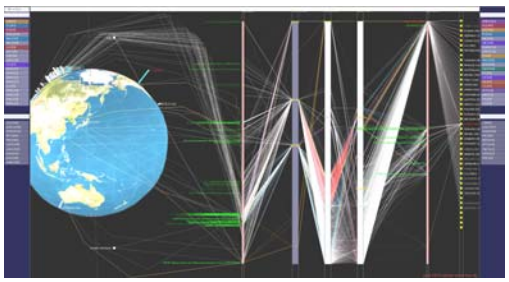
VisCat/Center는 관리하는 도메인의 트래픽만을 필터링하여 보여주는 화면으로써 (그림 7)과 같다. VisCat/Center에서는 관리하는 도메인에 존재하는 호스트의 물리적 위치를 GIS와 연계하여 2단계의 지리 정보 형태로 표현하기 때문에 네트워크 관리자는 이상현상이 발생한 위치를 쉽게 인지할 수 있다.



(그림 7) VisCat/Center

다. VisCat/Globe

VisCat/Globe는 전체 네트워크에서 발생하는 트래픽의 흐름을 표현하는 화면으로써 (그림 8)과 같다. VisCat/Globe는 한 화면에서 모든 프로토콜별 트래픽의 흐름을 파악할 수 있고, 목적지 및 근원지 포트별 빈도수가 막대그래프로 표현되기 때문에 이상현상을 파악하는 데 도움이 된다.

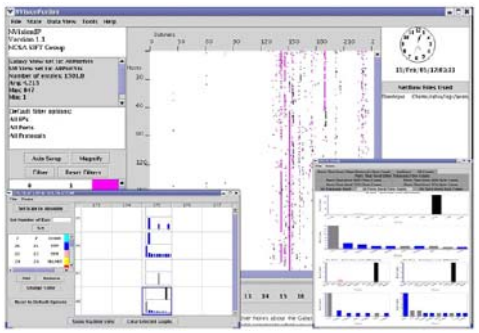


(그림 8) VisCat/Globe

VisCat은 트래픽의 연결선에 포트 번호에 따른 컬러를 매핑하여 연결 정보를 표현하고, 포트 번호별 사용 빈도수, 국가별 빈도수, ISP별 빈도수 등의 통계 정보를 한 화면에 표현함으로써 네트워크 관리자가 원하는 정보를 한 화면에서 모두 파악할 수 있는 장점이 있다. 따라서 VisCat의 경우 상세 정보를 얻기 위하여 다른 화면으로의 전환이 필요하지 않으며, 한 화면에서 클릭을 통하여 여러 가지 다양한 정보들만을 필터링하여 볼 수 있어 네트워크 관리자의 인지력을 향상시킬 수 있다. 또한 물리적 위치 정보를 제공하기 때문에 네트워크의 이상현상이 일어난 위치를 쉽게 파악할 수 있는 장점이 있다. 하지만 VisCat의 경우 VisFlowConnect-IP와 같이 임계값 이상의 이벤트만을 표시하지 않고, 모든 이벤트를 표현하기 때문에 관리자의 인지력은 저하될 수도 있다.

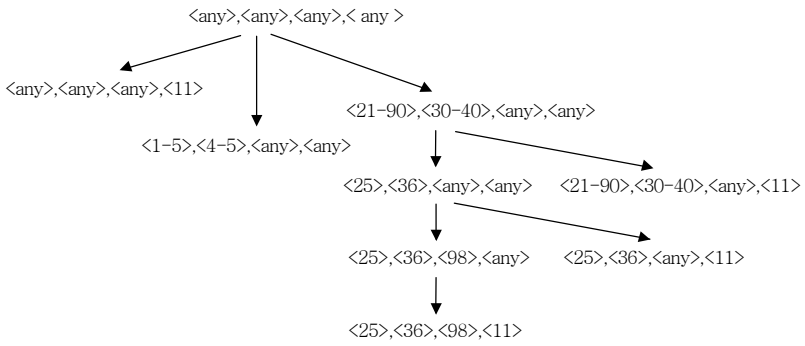
3. NVisionIP

NVisionIP(Closing-the-Loop)은 K. Lakkaraju et al.[5]에 의해서 제안된 위협 관리 목적의 보안 이벤트 시각화 기술이다. K. Lakkaraju et al. 등에 따르면 데이터로부터 관심이 있는 패턴을 찾는 과정을 발견(discovery)이라고 정의하고, 이러한 패턴과 동일한 인스턴스를 찾는 과정을 탐색(searching)이라고 정의할 때, 현재의 네트워크 보안 이벤트 시각화 기술은 패턴을 추출하는 과정에 초점을 맞추고 있다고 하였다. 하지만 네트워크 보안 이벤트 시각화 기술의 경우 단순히 보안 상황을 보여주는 것에 그치지 않고 이상 현상에 대한 대응을 하기 위해서는 발견 과정과 탐색 과정이 하나의 고리를 형성해야 한다고 주장하였다. 따라서 이 기술은 기존에 개발된 NVisionIP를 사용하여 관리자가 네트워크 공격에 대한 차단 규칙을 생성할 수 있도록 하였다.



(그림 9) NVisionIP[5]

NVisionIP의 경우 전체 네트워크 수준에 호스트별 유일한 포트의 사용 빈도수 등을 표현하는 Galaxy View, 사용자에 의해서 선택된 서브셋의 호스트별 플로 빈도수 등을 보여주는 Small Multi View,



(그림 10) 패턴 트리 예[5]

한 호스트의 트래픽의 통계 정보를 보여주는 Machine View의 세 가지 화면으로 구성되어 있으며, (그림 9)와 같다. (그림 9)에서 제일 위쪽의 화면이 Galaxy View, 왼쪽 하단의 그림은 Small Multiple View, 오른쪽 하단의 그림은 Machine View를 나타낸다.

NVisionIP의 세 화면에서 이상현상이 생긴 지점을 선택하게 되면 선택된 지점에 대한 패턴 트리가 형성되며, (그림 10)은 생성된 패턴 트리의 한 예이다. 이와 같이 관리자의 개입으로 생성된 패턴을 사용하여 침입탐지시스템 또는 방화벽 등과 연동하면 네트워크 공격을 빠르게 인지하고 차단할 수 있다.

앞에서 살펴본 것과 같이 현재 유선 네트워크에서의 보안 이벤트 시각화 기술은 많이 개발되고 있지만, 위협 관리를 목적으로 하는 시각화 기술은 이제 개발을 시작하는 단계이다. 현재 침입탐지시스템이 가지는 한계점을 극복하기 위해서는 보안 이벤트 시각화 기술이 꼭 필요하며 앞으로 알려지지 않은 공격, 제로데이 위협의 신속한 탐지 및 대응을 위해서 위협 관리를 목적으로 하는 시각화 기술이 더 많이 개발될 것으로 예상된다.

Ⅲ. 무선 네트워크에서의 시각화 기술

무선 네트워크의 사용자가 증가하면서 무선 네트워크에 대한 보안이 새로운 이슈로 떠오르고 있다. 무선 네트워크에서도 여러 가지 공격에 대한 탐지 기술이 개발되고 있지만, 유선 환경에서와 같이 분석해야 되는 이벤트의 양, 오탐률, 사용자의 편의성 등으로 인하여 앞으로 무선 네트워크에서도 보안 이벤트 시각화 기술을 중심으로 공격을 탐지하는 기술들이 개발될 것으로 예상된다. 무선 네트워크 환경에서의 보안 이벤트 시각화 기술은 무선 네트워크 상에서 발생하는 각종 정보들을 시각화하여 네트워크 관리자로 하여금 현재 네트워크의 보안 상황을 직관적으로 인지할 수 있도록 하는 기술이다. 현재 무선 네트워크에서의 시각화 기술은 무선 네트워크를 구성하는 중요 요소인 AP의 물리적 위치를 표현하고 정확한 네트워크의 범위를 시각화하는 무선 네트워크 매핑 기술과 무선 단말과 AP 간의 연결 정보를 표시하는 무선 네트워크 시각화 기술을 중심으로 연구가 진행되고 있다. 따라서 본 고에서는 무선 네트워크 매핑 기술과 무선 네트워크 시각화 기술로 나누어서 현재 개발되고 있는 기술의 동향과 앞으로의 기술 개발 방향에 대해서 논의할 것이다.

1. 무선 네트워크 매핑 기술

무선 네트워크 매핑 기술은 무선 네트워크의 정확한 범위를 시각화함으로써 네트워크 관리자가 현재 네트워크의 성능을 이해하는 데 도움을 준다. 또한 무선 네트워크 범위 평가, 보안 위협 탐지, rogue AP 탐지, hotspot 탐지, AP 설정 습관 측정 등에 사용될 수 있다[6]. 현재 무선 네트워크 매핑 기술은 사무실, 도서관, 실외에서 사용자의 휴대 단말의 위치를 표현하기 위해서 많이 개발되고 있으며, 위치 정보를 계산하는 데 사용되는 데이터에 따라서 GPS 기반과 RF 신호 기반으로 나눌 수 있다.

• GPS 기반 무선 네트워크 매핑 기법

GPS의 경우 전세계에서 사용할 수 있는 방법이며, 기존의 장비에 외장 동글, 외장 카드, 또는 유선 액세서리를 연결만 하면 사용할 수 있다. 현재 일반적인 GPS 기반의 방법은 10m의 정확도를 가진다고 알려져 있으며, 추가적인 정확도 증강 기법을 사용하면 정확도를 더 향상시킬 수 있다. 하지만 GPS의 경우에는 실내에서 사용할 수 없다는 단점이 있으며, 대도시의 경우에도 높은 빌딩 숲 때문에 GPS 수신의 영향을 받을 수 있다.

• RF 신호기반 무선 네트워크 매핑 기법

RF 신호를 사용하는 방법은 802.11 무선네트워크, GSM 데이터, 초음파, 적외선, 초광대역신호(UWB) 등을 사용하는 방법이 있다. 그 중에서 802.11 무선 네트워크를 구성하는 AP에서 생성되는 비컨 데이터를 사용하여 위치를 추적하는 방법이 가장 많이 연구되고 있다. 비컨 데이터를 사용하는 가장 대표

적인 방법으로는 RADAR 시스템[7]이 있으며, 1.5 미터의 정확도를 가진다.

현재 대부분의 무선 네트워크 매핑 기술은 802.11 무선 네트워크에서 AP와 호스트간의 수신신호강도(RSS)를 사용하는 방법을 중심으로 개발되고 있다. 수신신호강도의 경우 무선 네트워크 인프라로부터 획득하기 쉬우며, 위치 정보를 나타내는 가장 명백한 데이터이기 때문이다. 수신신호강도를 기반으로 하여 AP 및 휴대 단말의 위치를 표시하는 방법은 수신신호강도를 수집하는 방법과 수집된 정보를 사용하여 위치를 계산하는 방법에 여러 가지 방법이 존재한다. 수신신호강도를 수집하는 방법은 AP에서 정보를 수집하는 방법, 단말 호스트에서 정보를 수집하는 방법이 있다. 또한 최근에는 Yeung et al.[8]에 의해서 두 정보를 모두 수집하여 사용하는 방법이 개발되고 있으며, 이 경우에 기존보다 성능이 향상된다고 알려져 있다.

수신신호강도를 사용하여 위치를 계산하는 방법으로는 핑거프린트(fingerprints)를 사용하는 방법과 확률 분포(probability distribution)를 사용하는 방법이 있다. RADAR 시스템의 경우 핑거프린트를 사용하는 가장 대표적인 방법으로 알려져 있다. RADAR 시스템의 경우 단말 호스트에서 패킷을 브로드캐스팅한 후, AP가 수신하는 패킷에 대하여 수신신호강도를 계산하였다. 다른 방법들은 휴대 단말에서 수신신호강도를 추출하여 핑거프린트를 생성하였다.

확률 분포를 사용하는 방법의 경우 알려진 위치에서 측정된 수신신호강도들의 샘플을 사용하여 확률 모델을 생성한 후, 위치를 모르는 수신신호강도 샘플의 집합에 대하여 가장 확률이 높은 위치를 찾는 방법이다. Youssef et al.[9]에 의해서 제안된 HORUS 시스템, Xiang et al.[10]에 의해서 제안된 방법이 가장 대표적인 방법이며, 두 방법의 경우 모두 휴대 단말에서 획득된 수신신호강도를 사용하여 위치를 계산하였다.

무선 네트워크 매핑 기술을 사용하면 단순히 무선 네트워크 상태 정보만을 파악할 수 있으며, 네트워크의 보안과 관련된 정보를 표시해주지 못한다는 단점이 있다.

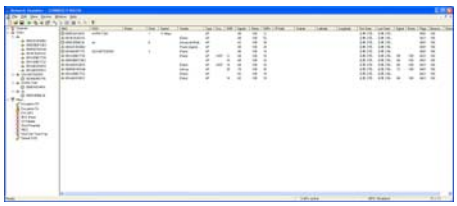
2. 무선 네트워크 시각화 기술

무선 네트워크 시각화 기술은 무선 네트워크를 통하여 이루어지는 트래픽 정보들을 화면상에 시각화함으로써 네트워크 관리자가 현재 무선 네트워크의 보안 상황을 이해하는 데 도움을 준다. 현재 무선 네트워크 시각화 기술의 경우 텍스트 또는 대시보드를 사용하는 방법들이 주를 이루고 있으며, 대표적인 방법들로는 Kismet, NetStumbler[11], WirelessMon[12], CommView for Wifi[13] 등이 있다. 텍스트 기반의 방법들은 주로 <표 2>와 같은 정보들을 텍스트 형태로 화면상에 표현한다. (그림 11)과 (그림 12)는 텍스트 기반의 대표적인 방법인 NetStumbler와 WirelessMon을 나타낸다. 이와 같은 방법들은 텍스트 기반의 표현 방법을 사용하기 때문에 한 화면에 표현할 수 있는 정보의 양에 제약이 있다. 따라서 네트워크 관리자는 필요한 정보를 찾기 위해서 여러 번 화면을 전환하거나, 화면을 스크롤 해야 되기 때문에 네트워크 관리자가 현재의 네트워크 상황을 직관적으로 인지하기에는 어려움이 있다.

IntraVUE[13], Wi-Viz[14], Wvis[15]의 경우 AP와 호스트의 연결 정보, 휴대 단말의 정보를 한 화면에 시각화하기 때문에 텍스트를 사용하는 방법

〈표 2〉 무선 네트워크 텍스트 정보

AP 정보	- SSID - 사용하는 채널 - 지원하는 속도 및 암호화 종류 - MAC 주소 - 신호 강도
채널 정보	- 채널을 사용하는 AP - 신호 강도 - 전체 패킷 수 - 프레임 종류별 패킷 수(관리, 데이터, 제어) - 각종 에러 관련(ICV 에러, CRC 에러 등)
패킷 정보	- 근원지, 목적지 IP 및 MAC 주소 - 사용하는 포트 및 프로토콜 - 시그널 강도 - 사용되는 AP 및 채널 정보



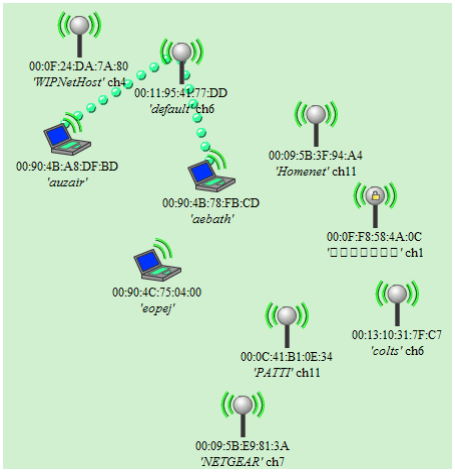
(그림 11) NetStumbler[11]

(그림 12) WirelessMon[12]

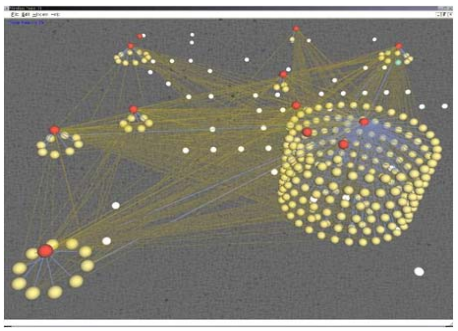
보다 한 화면에 표현할 수 있는 정보의 양이 많다. 또한 심볼, 아이콘, 색깔 있는 선 등을 사용하여 정보를 표현하기 때문에 네트워크 관리자가 현재의 네트워크 상태를 직관적으로 인지할 수 있는 장점이 있다. 하지만 무선 네트워크를 구성하는 호스트 및 AP의 개수가 많아지는 경우 인지력이 떨어지는 단점이 있다. (그림 13)과 (그림 14)는 시각화 표현 방법을 사용하는 무선 네트워크 시각화 방법 중 Wi-Viz와 WVis를 나타낸다. 이와 같은 방법들은 무선 AP를 중심으로 하여 AP에 연결된 호스트의 정보들을 시각화하였다.

현재까지 개발된 무선 네트워크 시각화 기술의 경우에는 AP의 정보, 호스트의 정보, AP와 호스트의 연결 정보 등 단순히 수집되는 데이터를 화면상에 표현하는 수준에 그치고 있다. 네트워크 관리자가 무선 네트워크 시각화 기술을 사용하여 현재 네트워크의 보안 상황을 인지하기 위해서는 AP와 호스트간의 트래픽, 채널별 트래픽 등을 시각화하여 보여주는 것이 필요하다.

무선 네트워크에서의 시각화 기술은 현재 새로운 이슈로 떠오르고 있지만, 아직 많은 연구가 더 필요



(그림 13) Wi-Viz[14]



(그림 14) WVis[15]

한 분야이다. 현재까지의 무선 네트워크에서의 시각화 기술은 무선 네트워크의 상태를 표현하기 위한 목적으로 개발되었지만, 앞으로는 무선 네트워크에서의 보안에 대한 요구사항이 많아지기 때문에 무선 네트워크의 보안 상황을 표현하기 위한 목적으로 개발될 것이다. 또한 무선 네트워크의 보안 상황을 인지하기 위해서 무선 네트워크 매핑 기술과 무선 네트워크 시각화 기술을 통합하여 물리적 공간상에 AP 및 휴대 단말의 실제 위치를 표현한 후, AP와 휴대 단말의 연결 정보뿐만 아니라 트래픽의 상세 정보를 시각화하는 방향으로 연구가 진행될 것이다.

Ⅳ. 결론

네트워크 보안 이벤트 시각화 기술은 제로데이

위협, 알려지지 않은 공격 등의 기존 기술이 가지는 한계점을 극복하기 위해서 활발한 연구가 진행될 것으로 기대된다.

앞으로의 유선 네트워크 환경에서의 보안 이벤트 시각화 기술은 네트워크에서의 이상현상 및 공격 패턴 분석 등의 보안상황 인지에 그치지 않고, 관리자의 개입으로 이상현상에 대한 대응 정책, 공격에 대한 차단 룰을 생성하는 방법을 제공하는 기술로 발전할 것이다. 이를 위해서는 방대한 양의 보안 이벤트를 실시간으로 분석하고, 기존의 패턴과 매칭할 수 있는 보안 이벤트 처리 기술의 개발이 필요할 것으로 예상된다.

무선 네트워크에서의 시각화 기술은 이제 초기 개발 단계이기 때문에 앞으로 더 활발한 기술 개발이 예상된다. 특히 현재에는 무선 네트워크 매핑 기술과 무선 네트워크 시각화 기술로 나누어져서 기술이 개발되고 있지만 앞으로는 두 기술을 통합된 형태의 기술이 등장할 것으로 예상된다. 새로이 등장할 기술은 AP 및 휴대 단말의 실제 위치를 지도 상에 표현하고, 이들간에 이루어지는 트래픽의 상세 정보를 시각화함으로써 유선 네트워크에서의 시각화 기술과 비슷한 방향으로 발전할 것이다. 무선 네트워크에서의 시각화 기술은 유선 네트워크에서 같이 궁극적으로 rogue AP 탐지, 채널, AP, 호스트 등에 대한 서비스 거부 공격, 분산 서비스 거부 공격 등의 다양한 위협을 탐지하고 차단할 수 있는 기술로 발전될 것이다.

● 용 어 해 설 ●

플로(Flow): 송신자와 수신자 호스트 간의 단방향의 패킷의 흐름을 의미하여, 패킷 단위의 트래픽을 aggregation 하여 생성한다. 플로를 생성하는 방법에 따라 Cisco Netflow, sFlow, cFlow 등이 있다.

약 어 정 리

AP	Access Point
GIS	Geographical Information System
GPS	Global Positioning System
RSS	Received Signal Strength
SSID	Service Set Identifier

참 고 문 헌

[1] 김재철, "DDos 공격 해결책은 IPS가 아니다," http://www.ddaily.co.kr/news/news_view.php?uid=37941, 2008.

[2] 장범환, 나중찬, 장종수, "시각화 기반의 네트워크 보안상황 인지 기술," 주간기술동향 1335호, 2008.

[3] K. Lakkaraju, W. Yurcik, and A.J. Lee, "NVisionIP: Netflow Visualizations of System State for Security Situational Awareness," *In Proc. of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ACM Press, New York, NY, USA, 2004, pp.65-72.

[4] Xiaoxin Yin, William Yurcik, and Adam Slagell, "The Design of VisFlowConnect-IP: A Link Analysis System for IP Security Situational Awareness," *Third IEEE Int'l Information Assurance Workshop*, University of Maryland, Mar. 23-24, 2005.

[5] Kiran Lakkaraju, Ratna Bearavolu, Adam Slagell, and William Yurcik, "Closing-the-Loop: Discovery and Search in Security Visualizations," *6th IEEE Information Assurance Workshop*, United States Military Academy at West Point, New York, June 2005.

[6] S. Byers and D. Kormann, "802.11b Access Point Mapping," *Communications of the ACM*, May 2003, pp.41-46.

[7] P. Bahl and V.N. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System," *In Proc. of IEEE Infocom 00*, Apr. 2000.

[8] W.M. Yeung and J.K. Ng, "Wireless LAN Positioning Based on Received Signal Strength from Mobile Device and Access Points," *In Proc. of the 13th IEEE Int'l Conf. on Embedded and Real-Time Computing Systems and Applications, IEEE Computer Society*, Washington, DC, 2007, pp.131-137.

[9] M. Youssef and A. Agrawala, "On the Optimality of WLAN Location Determination Systems," *TR UMIACSTR*, University of Maryland, College Park, Mar. 2003.

[10] Z. Xiang et al., "A Wireless Lan-based Indoor Positioning Technology," *IBM Journal of Research and Development*, Vol.48, 2004.

[11] Netstumbler, http://www.netstumbler.com/
[12] WirelessMon, http://www.passmark.com/
[13] Commview for Wifi, http://www.tamos.com/
[14] IntraVue, http://www.intravue.net/
[15] Wi-Viz, http://devices.natetrue.com/wiviz/