PCAV: 평행좌표계를 이용한 네트워크 공격의 시각화

최현상[0], 이희조
{realchs, heejo}@korea.ac.kr

PCAV: Parallel Coordinates Attack Visualizer

Hyunsang Choi[0], Heejo Lee
Dept. of Computer Science, Korea University.

요 약

인터넷상의 수많은 트래픽 정보 중에서 악성 트래픽 정보를 빠르게 감지하는 것은 그 정보의 방대함 때문에 쉽지 않다. 공격시각화(Attack Visualization) 기법은 이런 수많은 정보 중에서 악성 트래픽 정보를 좀 더 쉽게 인지하게 함으로써 새로운 공격에 대해서 빠른 대응과 피해 최소화를 하는데 활용할 수 있다. 본 연구에서는 평행좌표계(Parallel Coordinates)를 이용해 공격시각화를 하여, 분산 서비스 거부 공격, 웜, 스캐닝 공격 등 인터넷상에 알려진, 혹은 알려지지 않은 새로운 공격들에 대해 빠른 대응을 하기위한 기술 연구를 하였으며, 각 공격들의 특정 시각화 패턴을 감지하고 이를 알려주는 이상탐지(anomaly detection) 시각화 시스템 PCAV를 구현하였다. PCAV 시스템을 통해 네트워크 관리자는 실시간으로 트래픽 정보와 공격들의 시각화 정보를 원격에서도 모니터링하고 이를 통해 즉시 대응하는 것이 가능하다. 또한, 이전에 발생한 공격들의 시각화 정보를 확인하고 이를 분석하는 것과, 알려지지 않은 공격이 발생했을지라도 그 공격의 시각적 패턴이 나타났을 때 즉각 공격 서명(signature)으로 활용 하는 것이 가능하다.

1. 서 론

인터넷의 발달과 함께 급격한 사용자의 증가로 인해 오늘날의 네트워크는 복잡하고 다양한 종류의 트래픽들로 포화상태에 이르고 있다. 이러한 방대한 트래픽 데이터들을 효과적으로 분석하고, 악성 공격 트래픽에 대해 빠르게 인지, 대응하는 것이 중요하다. 그러나 수많은 정보 중에서 자신이 원하는 정보만을 빠르게 분석하고 탐지하는 것은 쉽지 않다. 이와 관련해 최근 정보시각화[1](Information Visualization)에 대한 연구가 활발히 진행되고 있으며, 그 목적과 방식에 따라 다양한 기법들이 개발되고 있다[2]. 정보를 시각화하면, 동일하지 않은 다양한 데이터들을 쉽게 다룰 수 있으며, 직관적 분석이 가능하여 빠른 대응이 가능하게 된다[3]. 또한, 시각화된 데이터들을 통해 새로운 가설을 유추하는 것도 가능하다. 본 연구는 이러한 정보시각화의 장점들을 활용하여 네트워크 보안 분야에 적용하고자 한다.

TCP/IP헤더에서 소스주소, 목적지주소, 목적지포트, 패킷길이와 같은 몇 가지 정보들을 이용하여 웜, DDoS공격, 스캐닝과 같은 인터넷 공격들에 대한 시각화를 할 수 있다. 본 연구에서는 시각화 기법 중 평행좌표계[4]를 사용하였다. 각 공격들이 평행좌표계서 상에서 시각화 되었을 때 나타나는 발산 량(divergence), 상관관계(correlation)와 같은 특징들을 통해 인터넷 공격들의 시각화 그래프 패턴을 찾고, 이를 이용해서 인터넷 공격들을 빠르게 감지하고 대응할 수 있게 하고자 한다. 특히, 현재 웜(알려진 혹은 알려지지 않은 신종 웜)의 시각화에 대한 연구를 중점적으로 진행하고자 한다.

연구에서 구현된 PCAV(Parallel Coordinates Attack Visualizer) 시스템은 실시간으로 동작하며, 특정 주기 동안 플로우 정보를 축적하여 분석-시각화 하는 작업을 한다. 시스템은 크게 분석모듈과 시각화모듈이 두 가지 부분으로 이루어져 있다. 분석 모듈은, 현재 일반화되고 있는 플로우[5] 기반의 분석 방법론을 바탕으로, 수집된 트래픽으로부터 플로우 정보를 생성하여 알고리즘을 거쳐 공격 트래픽 그룹들을 검출해 낸다. 시각화 모듈에서는 평행좌표계 방식을 통해 실시간으로 트래픽 데이터를 시각화 하고 분석 모듈에서 검출된 공격 트래픽 플로우의 그룹들을 리스트로 보여준 뒤 공격들 각각에 대해 따로 시각화한 그래프들을 그려준다.

2. 관련 연구

보안의 관점에서 시각화 기법을 적용한 예로를 CCV 기법이 있으며 이는 TCP/IP헤더의 세 가지 정보(source address, destination address, destination port)들을 이용하여 DDoS공격들과 스캐닝공격들을 3-D 그래프에 표현하였다[6]. 이 연구와 유사한 Shoki Packet Hustler 라는 2차원 혹은 3차원으로 시각화를 하는 오픈소스 프로젝트[7]도 진행되고 있다.

플래그 정보를 카운트하여 웜을 비롯한 DoS와 같은 인터넷 공격들을 탐지하고 시각화를 하는 Penn State University에서 사용하는 Ourmon[8]이라는 이상 탐지 시스템이 있다. 이 시스템에서 이상탐지 외에도 시각화를 제공하나 그 방식이 단순히 특정 플래그 수나 트래픽 양 혹은 패킷 수 등의 카운트 량을 바 그래프 형식으로 그래프를 그린 것으로 본 연구의 직관적 분석과 공격들의 패턴을 찾는 방식과는 차이가 있다.

이외에도 DoS 공격의 탐지와 대응, 그리고 웜의 전파 형태에 대하여 모델링을 하는 시도와 같은 이전 연구[9][10] 들이 존재하였다. 그러나 이 연구 들은 직관적인 인지를 위해 실시간으로 시각화를 하는 연구는 아니었다.

3. 공격시각화

공격시각화에서 시각화 기법 중 평행좌표계 방식을 사용하였으며, 평행좌표계에서 사용 할 인자(parameter) 값으로 TCP/IP 스택에서 소스주소, 목적지주소, 목적지포트, 그리고 패킷 길이로 정하였다. 나머지 헤더 정보들 중에서도 시각화에 사용할 수 있는 다른 필드 값들이 몇 가지 있으나 위에서 결정한 네 가지 값으로도 시각화 패턴이 잘 나타났기 때문에 사용하지 않았다. 평행좌표계는 2차원 평면에 3개 이상의 많은 수의 인자들 또한 쉽게 표현이 가능하며 이들의 발산 량, 추세(trend), 상관관계 또한 잘 나타나고[11], 2차원 평면이므로 다른 시각화 방식에 비교해 볼 때 구현도 쉽기 때문에 이번 시각화 연구에서 활용하게 되었다.

시각화할 인터넷 공격 중에서 먼저 웜을 살펴보자. 인터넷 웜은 불특정 다수 혹은 특정 취약성을 지닌 대상들에게 스스로 전파(자기 복제)를 하는 악성 프로그램이다. 즉, 하나의 웜 감염자가 불특정 다수의 대상에게 감염을 위한 웜 패킷 데이터를 보내는 것이다. 이런 웜의 특성 때문에 일반적으로 웜에는 전파대상의 주소를 랜덤 하게 만드는 부분이 포함 되어 있다. 이 특징을 소스 주소와 목적지주소 관계에서 본다면 일대다의(1:m)의 연결 구성이 이루어진다는 것을 의미한다. 슬래머 웜 트래픽 샘플데이터를 플로우 데이터로 가공한 뒤, 모든 플로우 정보를 위의 방식대로 평행좌표계에 표시를 하면 아래 그림 1과 같은

그래프가 나타난다. 아래 그래프의 독특한 패턴은 웜의 로컬 스캐닝 특징에 비롯한 것이다[12].

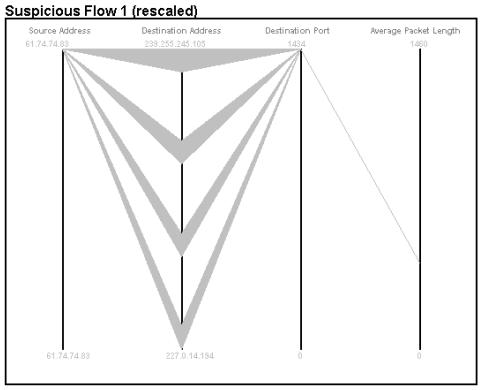

그림 1. 평행좌표계에서 슬래머 웜 트래픽.

분산 서비스 거부 공격의 경우 불특정 다수가 특정 목적지에 공격이 행해지는 경우가 일반적이기 때문에 이와 같은 경우 웜과는 반대로 목적지주소와 소스주소가 1:m 관계를 갖게 된다.

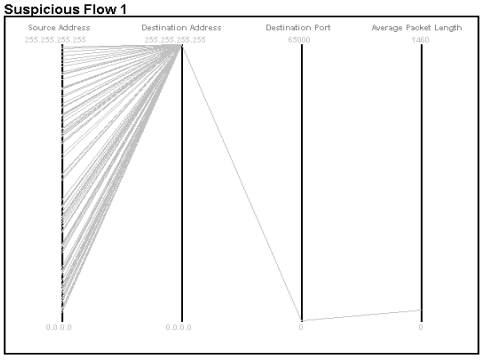

그림 2. 평행좌표계에서 DDoS 공격 트래픽.

이 그래프들에서 보는 바와 같이 공격 트래픽에서 소스주소, 목적지주소, 목적지포트, 평균패킷길이, 네 가지 인자 값들 사이에서 1:m의 관계 특성을 지니는 경우 평행 좌표축에서 이를 표현하면 특정한 그래프 패턴이 나타나게 된다. 이러한 그래프 패턴(signature)들을 정리하면 표 1과 같다.

Implied Attack	Signature	Divergences	Avg. Len
Portscan		1:1:m:1	48KB
Hostscan		1:m:1:1	48KB
Worm		1:m1:1	Not Fixed
Source-spoofed DoS[1]		m:1:1:1	48KB
Kamikaze		1:m:m:1	48KB
Source-spoofed DoS[2]		m:1:m:1	48KB
Distributed hostscan		m:m:1:1	48KB
Network-directed DoS		m:m:m:1	48KB
Single-source-spoofed DoS		1:1:1:1	48KB

표 1. Attack Signature

4. PCAV

본 연구에서는 PCAV(Parallel Coordinates Attack Visualizer)라는 시스템을 구축하였다. PCAV는 앞에서 언급한 공격시각화 기법을 이용하여 인터넷 공격에 대해 시각화를 하는 시스템으로서 플로우 기반의 모니터링 시스템으로 볼 수 있다. 트래픽 정보를 플로우 데이터로 가공하기 위해서 nProbe[13]라는 프로그램을 사용하였다. nProbe는 일정 시간 동안 트래픽 데이터를 축적하여 플로우 데이터로 가공한 뒤 PCAV 시스템에 이 데이터를 넘겨준다.

4.1 PCAV 시스템 구조

PCAV는 크게 분석모듈(Analyzer)와 시각화모듈(Visualizer)로 나뉜다. 전체 시스템의 구성도는 아래 그림 3과 같다.

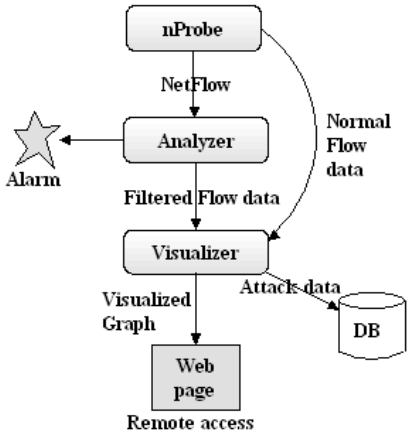

그림 3. PCAV 시스템 구성도

분석모듈에서는 nProbe로부터 받은 플로우 데이터를 읽어서 공격 데이터를 검출하여 각각을 그룹핑하고 특정 형태로 가공하여 시각화 모듈에 넘겨주는 역할과 공격 플로우가 감지되었을 때는 관리자에게 공격에 대해서 경고를 알리는 역할을 한다.

시각화모듈은 기본적으로 nProbe로부터 정상적인 플로우 데이터를 주기적으로 넘겨받아 이를 그림 4와 같이 평행좌표계에 그린다. 트래픽에 만약 공격으로 의심되는 데이터 그룹이 있는 경우 분석모듈이 이를 가공하여, 시각화모듈에 넘겨준다. 시각화모듈은 넘겨받은 공격그룹들을 리스트에 나타내어 주고 공격 그룹의 정보를 상태 창에 표시 한다. 사용자가 리스트에 나타난 공격 그룹 중 하나를 선택할 시에 선택된 공격그룹에 대해 그림 5처럼 평행좌표계 그래프를 그려준다. 좌표축의 값이 결정되어있는 경우 그 값의 분포에 대한 유추는 쉬우나 1:m의 연결에서 m의 값이 전체 좌표축의 크기에 비해 상대적으로 작은 경우 signature의 모양이 시각적으로 판단하기 힘들 수 있기 때문에 상대 좌표 값(최소값, 최대값으로 리스케일링)을 사용한 그래프도 같이 그려공격 그룹이 표시된 리스트를 클릭 할 때 이를 새로운 창에서 각각을 보여 준다. 공격 플로우 데이터는 데이터베이스로 저장이 되어 추후에 이 데이터를 읽어서 사용이 가능하게 하며, 시각화된 그래프들은 그림파일(png, gif)로 변환되어 서버의 웹 페이지에 자동 링크되어 원격에서도 관리자가 접근하여 실시간으로 그려지는 그래프와 공격 그래프를 확인 할 수 있게 한다. 여기서 PCAV가 설치된 PC가 웹 서버의 역할을 한다.

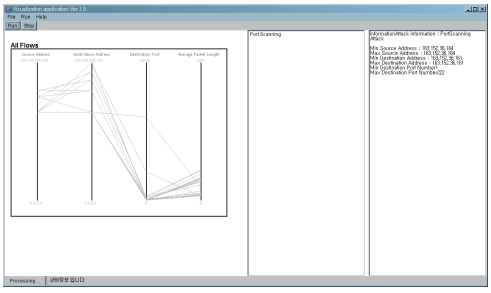

그림 4. PCAV 기본 인터페이스

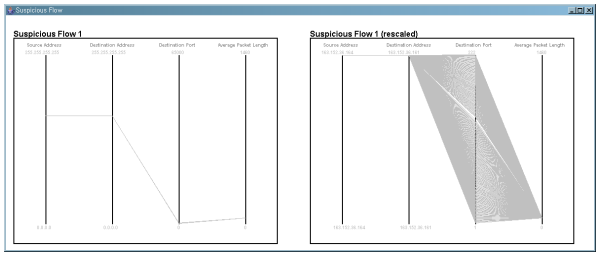

그림 5. 탐지된 포트스캔 공격시각화 그래프와 리스케일된 그래프

4.2 검사 알고리즘

분석모듈에서 공격 플로우 그룹들을 판별하기위해 검사 알고리즘을 사용한다. 알고리즘의 의사코드는 다음과 같다.

```
Attack_Detection( F_n ) F_n ← Flow data
1   F_j, F_{j+k} ← INPUT Flows contained in F
2   Temp_sa, Temp_da, Temp_dp ← I_j
3   FOR each j ≤ n
4      FOR each k ≤ n
5         IF DA_j = DA_{j+k} and DP_j = DP_{j+k}
6            DistSA[j]++
7            TempG_sa ← I_{j+k}
8         ENDIF
9         IF SA_j = SA_{j+k} and DP_j = DP_{j+k}
10           DistDA[j]++
11           TempG_da ← I_{j+k}
12        ENDIF
13        IF SA_j = SA_{j+k} and DA_j = DA_{j+k}
14           DistDP[j]++
15           TempG_dp ← I_{j+k}
16        EDNIF
17     ENDFOR
18     IF DistSA[j] > T ← Threshold
19        DDoS_list ← Temp_sa
20     ENDIF
21     IF DistDA[j] > T ← Threshold
22        IF AvgLen_temp < 50
23           Hostscan_list ← Temp_da
24        ELSE
25           Worm_list ← Temp_da
26        ENDIF
27     ENDIF
28     IF DistDP[j] > T ← Threshold
29        Portscan_list ← SusG_dp
30     ENDIF
31  ENDFOR
32  Count(SA_n), Count(DA_n), Count(DP_n)
33  IF Count(SA_n) > T or Count(DA_n) > T
       or Count(DP_n) > T
34        Abnormal ← TRUE
35  ENDIF
END of Attack_Detection
```

표 2. 검사 알고리즘

알고리즘에서 SA는 소스주소, DA는 목적지주소, DP는 목적지포트를 의미한다. I_j 는 j번째 플로우의 인덱스 이며, DistDA[j]는 j번째 플로우와 소스주소 목적지 포트가 같으면서 목적지 주소가 다른 플로우들의 카운트를 저장하는 배열이다. 나머지 DistSA[j], DistDP[j]도 마찬가지로 각각 소스주소 목적지포트에 대해 얼마나 분포된 값의 카운트를 저장하는 배열이다. Temp는 SA, DA, DP 각각에 대해 공격으로 의심되는 플로우들의 인덱스를 임시로 저장하는 장소이다. DDoS, Hostscan, Worm, Portscan 은 공격 플로우들의 인덱스를 Temp에서 넘겨받아 저장하는 공격 인덱스 배열의 리스트 이다.

현재 검사 알고리즘에서 판별이 가능한 공격은 5가지(웜, 포트스캔, 호스트스캔, DDoS 공격 1,2)이며, 나머지 공격에 대해서는 이상상태의 존재여부에 대해서만 판단이 가능하다. 나머지 공격들에 판별 알고리즘은 PCAV의 향후 연구로 진행할 예정이다.

검사 알고리즘에서 우선 n개의 전체 플로우들을 모두 입력받아서 하나씩 플로우 정보를 본다. 분석모듈에서 이 알고리즘을 적용하기 이전에 미리 데이터를 특정 형태 즉, 소스주소와 목적지주소, 목적지포트 세 값이 같은 플로우는 같은 플로우로 보고 이들을 합친 뒤 평균 패킷 길이 값을 갱신한다. 따라서 이 알고리즘에서 입력받는 플로우 정보들은 위에서 언급한 세 값이 동시에 같을 수 없기 때문에 이중 두 개의 인자 값이 같다면 나머지 하나의 인자 값은 반드시 다르다. 모든 플로우를 순서대로 비교를 해서 각 인자 값들에 대한 플로우 분포 수가 임계 값(Threshold) 넘은 경우에 1:m의 관계가 나타난 것으로 인식하여 공격 저장 배열 Temp에 기록되어 있는 그룹핑된 플로우들의 인덱스 값들을 공격 배열의 인덱스 저장 리스트들에 그 종류에 맞게 넘겨준다. 이외의 공격(동시에 두개 이상의 1:m 관계가 나타나게 되는 공격들)에 대한 검색 알고리즘은 개발 중이며, 현재 임시적으로 각 인자들에 대한 카운트를 해서(정렬 알고리즘을 이용) 이 값들 중 하나가 임계값을 넘는 경우에 이상상태로 판단, 다른 종류의 공격의 가능성을 경고하고 시각화 하도록 구성하였다. 알고리즘의 수행시간은 $O(n^2)$이다.

5. 결론 및 향후 연구

평행좌표계를 이용해 공격시각화를 하여 인터넷상에 알려진 각 공격들의 특정 시각화 패턴이 나타났으며, 이를 감지하고 알려주는 이상탐지 기반 시각화 시스템(anomaly-based visualization and detection system) PCAV를 구현하였다. PCAV 시스템을 통해 네트워크 관리자는 실시간으로 트래픽 정보를 시각화한 정보를 원격에서도 모니터링하고 PCAV가 알려주는 공격들의 시각화 정보를 통해 즉각 대응하는 것이 가능하다. 또한, 이전에 발생한 공격들의 시각화 정보를 확인하고 이를 분석하고 알려지지 않은 공격이 발생했을지라도 공격의 시각화 패턴이 나타났을 때 즉각 공격 서명으로 활용 가능하다.

향후 앞에서 언급한 모든 공격들에 대한 탐지 알고리즘 연구와 수행시간을 줄이는 방법의 연구, 웜의 종류에 따라 나타나는 시각적 패턴의 차이점을 분석하고, 앞으로 나타나게 될 새로운 형태의 웜과 그 외의 인터넷 공격들을 예측하여 이들의 시각화 특징과 이를 찾을 수 있는 알고리즘을 연구할 계획이다. 또한, 본 연구에서 사용하지 않은 다른 인자 값 들 중에서 플래그의 경우는 시각화에 적용하기 좋은 특징을 지니기 때문에 향후 시각화 시스템(PCAV)에 적용을 고려하고 있다.

6. 참고 문헌

[1] www.infovis.org
[2] Information Visualization and Visualization Techniques, http://pfp7.cc.yamaguchi-u.ac.jp/~ichikawa/iv/
[3] D. Keim, "Visual exploration of large databases," Communications of the ACM, vol. 44, no. 8, pp. 38-44, 2001.
[4] Inselberg, Alfred. "The plane with parallel coordinates." The Visual Computer 1. Springer, 1985, pp 69-91.
[5] Cisco netflow. http://www.cisco.com/warp/public/732/Tech/netflow
[6] Hyogon Kim, Inhye Kang, and Saewoong Bahk, "Real-time Visualization of Network Attacks on High-speed Link", IEEE Network Magazine, Sept.-Oct. 2004.
[7] http://shoki.sourceforge.net/hustler/
[8] http://ourmon.cat.pdx.edu/ourmon/info.html
[9] M. Garetto, G. Gong, and D. Towsley, "Modeling Malware Spreading Dynamics," Proc. IEEE INFOCOM 2003, Mar. 2003.
[10] D. Moore et al., "Internet Quarantine: Requirements for Containing Self-Propagating Code," Proc. IEEE INFOCOM 2003, Mar. 2003.
[11] Girardin L. and Brodbeck D. "A Visual Approach for Monitoring Logs". In Proceedings of the 12th System Administration Conference (LISA '98), pages 299-308, Boston, MA, December 1998.
[12] Evan Cooke, Z. Morley Mao, Farnam Jahanian, "Worm Hotspots: Explaining Non-Uniformity in Worm Targeting Behavior", University of Michigan, November 12, 2004
[13] http://www.ntop.org/nProbe.html