네트워크 트래픽을 이용한 사이버공격 발생원 추적방법

이수강, 김성민, 구영훈, 김명섭

고려대학교

{sukanglee, gogumiking, gyh0808, tmskim}@korea.ac.kr

Tracking Method about Cyber Attack Source using Network Traffic Data

Su-Kang Lee, Sung-Min Kim, Young-Hoon Goo, and Myung-Sup Kim

Korea Univ.

요 약

오늘날 인터넷으로 연결된 세상은 그물망처럼 정교해지고 있으며 이러한 환경은 소위 사이버 테러범로 불리는 사이버 공격자들에게 더없이 좋은 공격 환경을 제공해주고 있다. 이러한 이유로 악성행위 및 공격트래픽 탐지는 업계와 학계에서 동시에 많은 요구사항을 받고 있으며 네트워크 모니터링 분야에서는 사이버 공격트래픽을 찾아내려는 많은 연구들이 이루어지고 있다. 하지만 사이버 공격트래픽은 매 공격마다 알려지지 않는 새로운 형태의 트래픽이 발생하며 이는 공격트래픽 탐지를 어렵게 한다. 본 논문에서는 네트워크 트래픽에서 악성행위로 의심되는 정보를 바탕으로 공격트래픽의 발생원을 추적하는 방법을 제안한다. 제안하는 방법은 발생한 플로우 사이의 연결성과 유사성을 계산하여 연속적으로 발생하는 유사한 플로우를 역으로 추적하는 방법이며 이를 위해 FCI(Flow Correlation Index)를 정의하고 이를 사용한 HSC(Hybrid Similarity and Connectivity) 알고리즘을 제안하였다. 본 논문에서 제안한 사이버공격 트래픽 발생원 추적방법을 실제로 발생했던 여러 가지 사이버 공격 트래픽에 적용한 결과 신뢰할 만한 수준의 결과를 얻을 수 있었다.

Ⅰ. 서 론

오늘날 인터넷으로 연결된 세상은 그물망처럼 정교해지고 있으며 이러한 환경은 소위 사이버 테러범으로 불리는 사이버 공격자들에게 더없이 좋은 공격 환경을 제공해주고 있다. 이러한 환경적 요인은 사이버 공격이 급격히 증가하게 된 원인중 하나이며 사이버 악성행위 및 공격트래픽 탐지는 업계와 학계에서 동시에 많은 요구사항을 받고 있는 상황이다. 특히 네트워크 모니터링 분야에서는 공격트래픽을 찾아내려는 연구들이 이루어지고 있지만 사이버 공격트래픽은 매 공격마다 새로운 형태로 공격이 이루어지기 때문에 악성행위를 포함하는 비정상 트래픽의 탐지는 쉽지 않은 실정이다.

최근 트래픽의 통계정보를 기반으로 트래픽 형태를 분류하는 다양한 기준들이 제시되었으며 대표적으로 관련연구[1]에서는 플로우의 크기, 발생시간, 발생 빈도와 같은 통계정보를 이용하여 트래픽을 그룹핑하고, 분류하는 연구가 진행되고 있다. 이러한 그룹핑 방법은 트래픽의 발생 형태를 특징화하기 때문에 트래픽 분류에 용이하게 사용되고 있다. 본 연구에서는 인터넷에서 발생하는 트래픽들 중 플로우의 헤더정보(IP, Port, Protocol)와 통계정보(패킷 크기, 방향등)를 이용하여 악성트래픽이라 의심되는 최초 정보로부터 발생된 트래픽을 연속적으로 그룹핑하여 악성트래픽의 발생원을 추적하는 방법을 제시한다. 발생원을 추적하기 위해 두 플로우 간 연결성(Connectivity)과 유사성(Similarity)를 수치화 할 수 있는 FCI(Flow Correlation Index)를 정의한다.

본 논문에서는 2장에서 악성트래픽이라 판단되는 플로우를 그룹핑 하기 위한 FCI값을 정의하고 발생원을 추적하기 위한 방법론을 설명하며 3장에서는 본 논문에서 제시한 방법론의 성능을 입증하기 위해 실제 사이버 공격이 이루어지는 시점의 트래픽에 추적 방법을 적용한 실험 결과를 기술한다. 마지막으로 4장에서는 결론과 향후 연구 과제를 기술한다.

이 논문은 BK21 플러스 사업(No. T1300573), 2015년도 정부(교육부)의 재원 한국연구재단의 기초연구사업(No.2015R1D1A3A01018057), 2015년도 정부(미래창조과학부)의 재원 정보통신기술진흥센터 지원(No.B0101-15-0300)을 받아 수행된 연구임.

Ⅱ. 연구 내용

본 장에서는 악성트래픽이라 판단되는 플로우를 그룹핑하기 위한 FCI(Flow Correlation Index)를 정의하고, 악성트래픽의 발생원을 추적하는 방법을 설명한다.

최근에 사이버 상에서 가장 많은 위협의 사이버 공격은 지능형 지속공격(APT, Advanced Persistent Threat)[2]이다. APT 공격은 특정 타겟에 대한 지능적이고 지속적인 위협으로 정의할 수 있다. 실제로 이란의 핵 정유시설을 공격했던 스턱스넷과 같은 사례를 참고하면 한번의 APT 공격을 위해 30억 이상의 비용과 3개월 이상의 시간을 투자했을 것이라고 한다. 이처럼 APT공격의 특징은 특정 시스템이나 네트워크 장비등의 핵심 장비에서 기존에 알려지지 않은 취약점을 이용해 타겟 네트워크나 시스템에 침입하여 공격하는 것이다. APT 공격은 시스템에 침투하여 공격을 바로 진행하는 것이 아니라, 침투 후 전체 시스템에 대한 전반적인 구조를 파악한 다음 유용한 데이터를 수집한다. 마지막 단계로 수집한 정보를 유출함과 동시에 해당 시스템의 운영을 방해하거나 장비를 파괴하게 된다. 이처럼 APT공격은 여러 단계를 거쳐 공격을 실행하게 되며, 이는 네트워크 트래픽으로 나타나게 된다. 이렇게 네트워크 트래픽에서 공격 트래픽 플로우들의 시간 순차적 흐름을 찾는 플로우 상관값이 FCI (Flow Correlation Index) 이다.

FCI는 사용자에게 입력받은 공격의 최초 정보를 바탕으로 찾아낸 최초 그룹과 비교되는 플로우간의 연결성과 유사성을 계산하여 정의된다. 연결성(Connectivity)은 두 플로우간 시작시간과 5-Tuple(SIP, SPort, DIP, Dport, Protocol) 총 6개의 속성값을 이용하여 계산되며 연결성을 계산하는 공식은 아래 수식 1과 같다. 유사성(Similarity)은 플로우의 통계정보 중 플로우에 포함된 N개까지의 패킷의 크기를 Cosine Similarity를 이용해 계산된다. 본 논문에서는 최대 5개까지의 패킷 크기를 사용하였으며 유사성을 계산하는 공식은 아래 수식 2와 같다. PFCI(Primitive-FCI)는 두 플로우간의 연결성과 유사성에 각각 가중치 값을 곱한 결과를 합한 값이며 수식 3은 PFCI를 계산하는 수식을 나타낸 것이다.

수식(1) $Conn(f_x,f_y)=\sum_{i=1}^{6}(w_i\times a_i(f_x,f_y))$

수식(2) $Sim(f_x,f_y)=\frac{f_x\cdot f_y}{\|\overrightarrow{f_x}\|\cdot\|\overrightarrow{f_y}\|}$

수식(3) $PFCI(f_x,f_y)=w_c\times Conn(f_x,f_y)+w_s\times Sim(f_x,f_y)$

1. HSC(Hybrid-SimilarityandConnectivity)FCI추적방법

본 논문에서는 공격원인의 추적은 PFCI가 아닌 HSC-FCI 추적 방법을 사용한다. HSC(Hybrid-Similarity and Connectivity)-FCI 추적방법은 PFCI와 같이 두 플로우간의 연결성(Con)과 유사성(Sim) 계산 값을 동시에 사용하는 것이 아니라 연결성과 유사성 계산된 값을 번갈아 가면서 사용한다.

$$SeedInfo=\{SrcIP, SrcPort, DstIP, DstPort, Protocol, TimeInfo\}$$

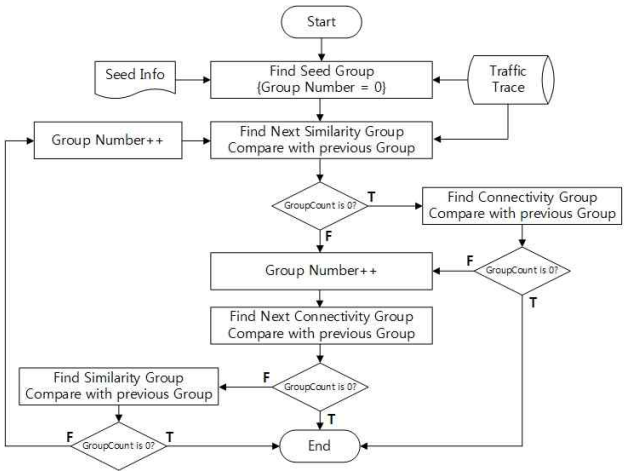

그림 1. Hybrid-Similarity and Connectivity 알고리즘 순서도

그림 1은 HSC-FCI 추적 방법의 알고리즘을 순서도로 표현한 그림이다. 사용자에게 최초로 입력받은 Seed Info(그림 1의 상단에 표기한 정보)를 바탕으로 전체 트래픽 트레이스에서 Seed Group을 찾고, Seed 그룹과 유사성(Sim)을 계산하여 계산한 값이 임계치를 만족하는 플로우를 그룹핑 한다. 그룹핑 된 플로우를 기준으로 연결성(Con)을 계산하여 계산한 값이 임계치를 만족하는 플로우 또한 그룹핑 한다. 이와 같이 시드 그룹으로부터 임계치를 만족하는 연속된 플로우들을 그룹핑 하게 된다. 만약 연속적으로 두 번 이상 그룹핑 된 플로우가 없는 경우에는 더 이상 그룹핑 되는 플로우가 없다는 것이므로 그룹을 찾는 과정을 종료한다.

Ⅲ. 실험 결과

본 장의 실험에서 사용하는 트래픽은 2013년 3월 20일부터 발생한 "320 대란" 때의 과정을 시뮬레이션 하면서 수집한 트래픽 트레이스다. 트래픽 트레이스에는 실제 APT공격의 과정이 단계별로 반영되었으며, 본 논문에서 제안한 HSC-FCI 추적방법을 사이버공격이 이루어지는 시점의 실제 트래픽에 적용하여 그 성능을 검증하였다.

그림 2는 실험에 사용되는 트래픽 트레이스의 공격 시나리오를 나타낸 것이며, 공격 과정은 총 7단계로 걸쳐 진행되었다. 그림 2에서 나타낸 ① 번부터 ⑦번까지의 공격에 사용된 플로우의 개수는 26개이며 표 1은 전체 트래픽과 공격에 사용된 트래픽의 정량적 수치를 나타낸 것이다. 공격에 사용된 플로우는 전체 플로우의 0.1%(패킷과 바이트는 전체의 0.3%)를 차지하고 있으며, 공격트래픽은 전체 트래픽 중에서 매우 낮은 비율을 차지하고 있는 것을 알 수 있었다.

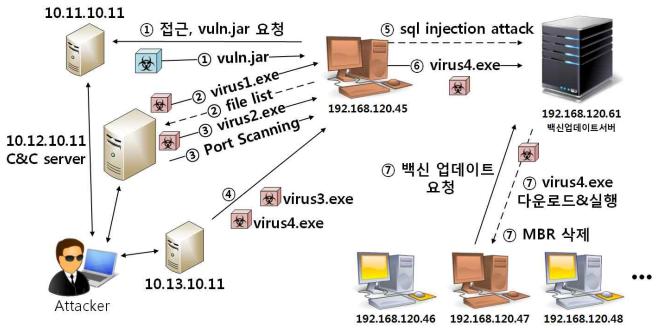

그림 2. 실험에 사용된 APT 공격 시나리오

	Flow	Packet	Byte(KB)
Total Traffic	15,459	193,574	108,144
Attack Traffic	26	640	430

표 1. 실험에 사용된 트래픽의 정량적 정보

표 2는 제안하는 사이버 공격 트래픽의 추적 방법의 성능을 검증하기 위해 연결성, 유사성, 그리고 시간정보의 임계값을 변경하면서 진행한 실험 결과를 나타낸 것이며 Precision(정확도)과 Recall(분석률)을 이용하여 성능을 평가하였다. 실험에 사용된 Seed Info는 ⑦번 시나리오의 SIP(192.168.120.46), DIP(192.168.120.61)를 사용하였다.

Threshold			Precision	Recall
Con	Sim	Time		
0.71	1.0	30	78.79%	100%
0.71	1.0	25	81.25%	100%
0.71	1.0	20	92.86%	100%
0.71	0.5	20	1.03%	100%
0.65	1.0	30	68.42%	100%
0.6	0.5	30	0.43%	80.77%

표 2. 사이버 공격 트래픽 추적 실험 결과

실험 결과 플로우의 연결성과 유사성을 기준으로 사이버공격 트래픽를 추적하는데 최대 92.86%의 정확도와 100%의 분석률에 달하는 성능을 보였다. 결과적으로 본 논문에서 제안하는 HSC-FCI 추적 방법을 이용하여 전체 트래픽에서 상대적으로 적은 양의 사이버 공격트래픽을 성공적으로 추적할 수 있다는 것이다.

Ⅳ. 결론 및 향후 연구

본 연구에서는 전체 트래픽에서 사이버 공격트래픽을 추적하는 방법을 제안하였다. 해당 방법 사용하면 사용자에게 Seed Info를 입력받고, 입력받은 정보로 Seed Group을 만들게 된다. 이 후 생성된 Seed Group과 나머지 플로우들과의 연결성, 유사성을 계산하여 최종적으로 공격이라 의심되는 트래픽을 추적할 수 있게 되는 것이다. 본 논문에서 제안한 방법을 실제 사이버 공격 트래픽에 적용한 결과 전체 트래픽중 플로우 기준 0.1%를 차지하는 적은 양의 공격 트래픽을 최대 92.86%의 정확도와 100%의 분석률로 찾아낼 수 있었다. 결과적으로 본 논문에서 제안한 방법을 사용하면 공격플로우를 찾아낼 수 있다는 것이다. 향후 연구로는 본 논문에서 제안한 방법을 응용한 사이버 공격추적 시스템을 연구할 예정이다.

참 고 문 헌

[1] An, Hyun-Min, et al. "Traffic Identification Based on Applications using Statistical Signature Free from Abnormal TCP Behavior." Journal of Information Science & Engineering 31.5 (2015).

[2] Kim, Yong-Ho, and Won Hyung Park. "A study on cyber threat prediction based on intrusion detection event for APT attack detection." Multimedia Tools and Applications 71.2 (2014): 685-698.