# 사이버 블랙박스에 기반한 공격 원인 분석 알고리즘

최선오, 이주영, 최양서, 김종현, 김익균
전자통신연구원 네트워크보안연구실
e-mail : suno@etri.re.kr

# Attack Cause Analysis Algorithm using Cyber BlackBox

Sunoh Choi, Jooyoung Lee, Yangseo Choi, Jonghyun Kim and Ikkyun Kim
Network Security Research Group, ETRI

**요 약**

요즘 인터넷을 통하여 많은 사이버 공격이 일어나고 있다. 이에 대응하기 위하여 우리는 네트워크 패킷을 저장할 수 있는 사이버 블랙박스 시스템을 개발하고 사이버 블랙박스 시스템에서 수집한 많은 네트워크 패킷을 분석할 수 있는 효율적인 공격 원인 분석 알고리즘을 제안한다. 공격원인 분석 알고리즘을 통하여 우리는 사이버 공격에 발생했을 때 공격의 유입점이 어디이고 어떤 경로를 통해서 공격이 이루어졌는지 알 수 있다. 그 뿐만 아니라 숨겨진 피해자 발견 알고리즘을 통하여 알려진 피해자뿐만 아니라 알려지지 않은 다른 피해자를 찾을 수 있다.

## 1. 서론

인터넷이 발달함에 따라 네트워크 상에서 많은 사이버 공격이 발생하고 있다. 이에 따라 네트워크 포렌식이 많은 관심을 받고 있다. [1] 그리고 네트워크 포렌식을 위하여 네트워크 로그를 저장하고 분석하는 일들이 이루어져왔다. [2] 그러나 네트워크 로그 정보만으로는 네트워크 포렌식을 효과적으로 수행하는데 어려움이 있었고 네트워크 패킷을 저장할 필요성이 제기되어왔다. 이에 우리는 네트워크 포렌식을 위하여 네트워크 패킷을 캡쳐하고 저장하는 사이버 블랙박스 시스템을 개발하고 있다.

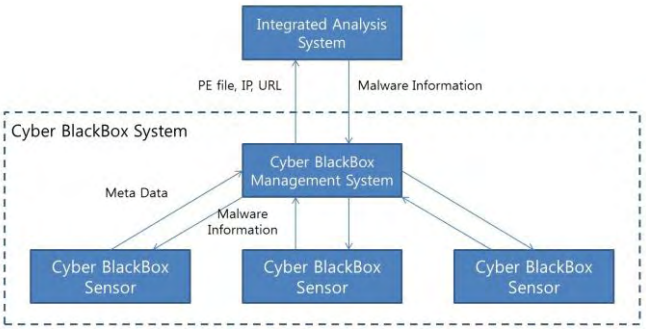
그러나 현재의 고속 네트워크 상에서 네트워크 패킷을 수집하는 것은 엄청난 양의 데이터로 인하여 분석의 어려움이 뒤따른다. [3] 이러한 문제를 해결하기 위하여 우리는 효율적으로 수많은 네트워크 패킷 데이터를 분석할 수 있는 공격 원인 분석 알고리즘을 필요로 한다. [4] 공격 원인 분석 알고리즘을 통하여 우리는 공격에 사용된 다른 호스트들을 발견하고 공격 원인을 파악하여 차후에 유사한 다른 공격을 대비할 수 있도록 한다.

이 논문에서는 사이버 블랙박스 시스템의 개념을 소개하고 사이버 블랙박스 시스템이 수집한 수많은 네트워크 패킷 데이터들로부터 효율적으로 공격 원인을 분석하는 알고리즘을 제안한다. 추가적으로 알려진 피해 시스템 뿐만 아니라 알려지지 않은 피해 시스템을 찾는 알고리즘을 제안한다. 마지막으로 시뮬레이션을 통하여 우리가 제안한 알고리즘들이 적절한 성능을 가지고 있음을 보여준다.

이 논문은 다음과 같이 구성된다. 2 장에서는 사이버 블랙박스 시스템의 개념을 소개하고 3 장에서는 효율적인 공격 원인 분석 알고리즘을 제안한다. 그리고 4 장에서는 알려지지 않은 다른 피해시스템을 찾는 방법을 제안하고 5 장에서는 시뮬레이션 결과를 보여준다. 그리고 마지막으로 6 장에서는 결론을 제공한다.

## 2. 사이버 블랙박스 시스템 구조

사이버 블랙박스 시스템은 그림 1 과 같이 크게 사이버 블랙박스와 통합분석시스템으로 구성된다. 그리고 사이버 블랙박스는 사이버 블랙박스 센서와 사이버 블랙박스 관리시스템으로 구성된다.




(그림 1) 사이버 블랙박스 시스템 구조도

사이버 블랙박스 센서는 그 센서가 설치된 네트워크 상의 네트워크 패킷을 캡쳐하고 저장하는 장치이다. 10Gbps 대역폭의 네트워크 상의 네트워크 패킷을 저장할 수 있는 장치이다. 이것을 위하여 특별한 하드웨어 장치를 사용하고 대용량의 하드디스크에 네트워크 패킷을 저장한다. 그리고 네트워크 패킷들로부터 전송되는 실행파일을 추출하는 모듈을 가지고 있고 고속검색을 위하여 인덱스와 증거보존을 위하여 무결성을 보장하는 모듈을 가지고 있다.

사이버 블랙박스 관리시스템은 여러 개의 사이버

블랙박스 센서로부터 메타 데이터를 받아 보관하고 있다. 메타 데이터는 네트워크 로그, 인덱스, 실행파일 등이 해당된다. 그리고 사이버 공격이 발생했을 때 메타 데이터를 기반으로 공격원인분석을 할 수 있는 기능을 가지고 있다.

통합분석시스템은 실행파일이 주어졌을 때 그 실행파일이 악성파일인지 분석할 수 있는 기능을 가지고 있다. 그리고 여러 개의 사이버 블랙박스 관리시스템과 연결되어 통합분석의 기능을 제공한다.

사이버 블랙박스 센서와 관리시스템의 연동은 다음과 같이 이루어진다. 사이버 블랙박스 센서는 네트워크 패킷을 저장하고 네트워크 패킷 로그와 인덱스, 실행파일 같은 메타데이터를 관리시스템에 제공한다. 그리고 사이버 블랙박스 관리시스템은 악성파일정보와 악성호스트의 IP 주소와 URL 과 같은 정보를 사이버 블랙박스 센서에게 제공한다.

그리고 사이버 블랙박스 관리시스템과 통합분석시스템은 다음과 같이 동작한다. 관리시스템이 실행파일, IP, URL 의 정보를 통합분석시스템에 주면 통합분석시스템은 악성파일분석을 통해 그 실행파일의 악성여부를 판단한다. 그리고 그 악성실행파일을 전송한 호스트의 IP 나 URL 의 정보를 그 관리시스템을 포함한 여러 다른 관리시스템에 제공한다.

### 3. Reverse Cause Analysis Algorithm (RCA)

이 단락에서는 효율적으로 공격원인을 분석하는 RCA 알고리즘을 제안한다. 사이버 블랙박스 시스템을 통하여 우리는 수많은 네트워크 패킷 정보와 실행파일 정보를 가지고 있다. 그 가운데 우리가 공격원인분석을 위하여 사용할 수 있는 정보는 사이버 블랙박스 센서가 수집한 네트워크 패킷 정보와 피해시스템 정보이다. RCA 알고리즘은 다음과 같다.

**RCA 알고리즘**

Input : 네트워크 패킷 정보, 피해시스템정보

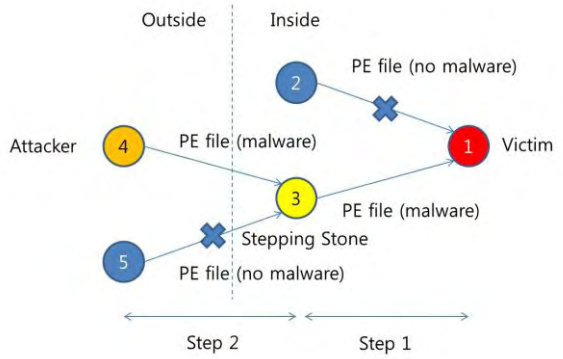
Output : 공격자와 중간자 정보

1: 피해시스템이 받은 실행파일을 찾고 그 실행파일을 통합분석시스템에 보낸다.

2: 통합분석시스템은 실행파일의 악성여부를 분석하고 결과를 사이버 블랙박스 관리시스템에 보낸다.

3: 관리시스템은 악성파일을 보낸 노드를 찾는다.

4: 1 에서 3 의 과정을 더 이상의 새로운 노드를 찾을 수 없을때까지 반복한다.




(그림 2) 역방향 원인분석 알고리즘

RCA 알고리즘의 예는 그림 2 와 같다. 노드 1 이 피해시스템이라는 것이 알려졌다고 가정한다. 그리고 노드 1 은 노드 2 와 노드 3 으로부터 실행파일을 받았다. 그리고 사이버 블랙박스 관리시스템은 그 실행파일들을 통합분석시스템에게 보낸다. 통합분석시스템은 첫번째 실행파일은 악성이 아니고 두번째 실행파일은 악성이라고 판단한다. 두번째 단계에서 관리시스템은 노드 3 이 공격의 중간자나 공격자로 사용되었다고 판단한다. 그리고 노드 3 은 노드 4 와 노드 5 로부터 실행파일을 받았다. 그래서 관리시스템은 그 실행파일들을 통합분석시스템에게 보내고 통합분석시스템은 첫번째 실행파일은 악성이고 두번째 실행파일은 악성이 아니라고 분석한다. 노드 4 는 외부 네트워크에 존재하는 호스트이므로 더 이상의 분석을 수행할 수 없다. 따라서 노드 4 가 공격자나 중간자로 사용되고 노드 3 은 중간자로 사용되었다고 분석한다.

### 4. Hidden Victim Detection Algorithm (HVD)

우리는 RCA 알고리즘에서 피해시스템이 알려져 있다고 가정하였다. 그러나 알려지지 않은 또다른 피해시스템이 존재할 수 있다. 알려지지 않은 또다른 피해시스템을 찾는 것을 통하여 우리는 차후의 또다른 공격을 막을 수 있다. 이 목적을 위하여 우리는 HVD 알고리즘을 제안한다. 그 알고리즘은 다음과 같다.

**HVD 알고리즘**

Input: 네트워크 패킷 정보, 피해시스템정보, 공격자/중간자 정보

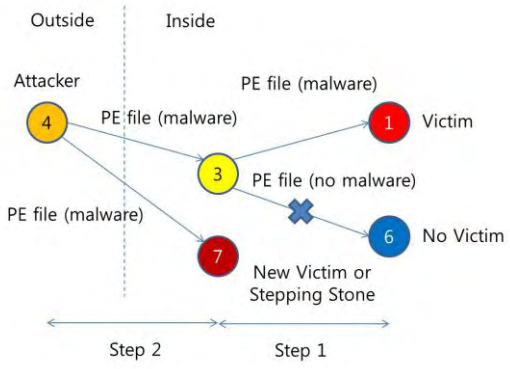
Output: 알려지지 않았던 새로운 피해시스템정보

1: 중간자와 공격자 정보는 큐에 저장되어 있다. 큐에서 하나의 노드를 꺼내고 그 노드가 다른 노드로 보낸 실행파일을 찾아 통합분석시스템에 보낸다.

2: 통합분석시스템은 실행파일의 악성여부를 관리시스템에게 알려준다.

3: 악성파일을 받은 새로운 노드는 새로운 중간자나 피해자가 되고 그 노드정보를 큐에 넣는다.

4: 1 에서 3 의 과정을 더 이상의 새로운 노드를 찾을 수 없을 때까지 반복한다.




(그림 3) Hidden Victim Detection 알고리즘

HVD 알고리즘의 예는 그림 3 과 같다. RCA 의 알고리즘을 통해 우리는 노드 3 이 중간자이고 노드 4 가 공격자임을 분석하였다. 노드 3 은 노드 1 외에 노

드 6 으로 실행파일을 보냈고 그 실행파일은 통합분석시스템에서 악성이 아닌 것으로 분석되었다면 노드 6 는 피해자가 아니라고 분석한다. 그리고 큐에서 노드 4 를 꺼내고 노드 4 는 노드 3 뿐만 아니라 노드 7 에도 실행파일을 보냈다. 그리고 그 실행파일은 악성이라고 분석되면 노드 7 을 중간자나 피해자라고 분석하고 노드 7 의 정보를 큐에 넣는다. 노드 7 에서 더 이상 실행파일을 다른 노드로 보내지 않았으면 알고리즘을 종료한다.

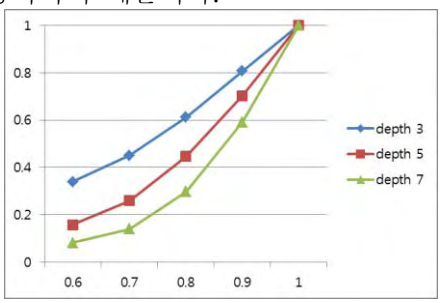
## 5. 실험결과

### 5.1 실험환경

우리는 시뮬레이션을 통하여 우리의 알고리즘들이 어느 정도의 성능을 가지고 있는지 확인한다. 전체 네트워크 노드의 수의 1000 개이고 통합분석시스템이 사이버 블랙박스로부터 실행파일을 받고 그 실행파일이 악성파일임을 분석하는 정확도를 0.6~1.0 으로 설정한다. 그리고 각 공격자가 공격하는 경로의 길이를 depth 라고 하고 3~7 로 설정한다. 그리고 각 공격자는 인접한 2 개의 노드를 공격하는 것으로 가정한다. 우리는 두가지 변수를 가지고 있다. 하나는 통합분석시스템의 악성파일분석정확도이고 다른 하나는 공격경로길이이다. 그리고 우리는 두가지 시뮬레이션을 하는데 첫번째 시뮬레이션을 RCA 알고리즘을 사용하여 천번의 실험을 수행하였을 때 공격자를 찾는 비율을 보여준다. 두번째 시뮬레이션은 HVD 알고리즘을 사용하여 알려지지 않은 다른 피해자 노드를 찾는 비율을 보여준다.

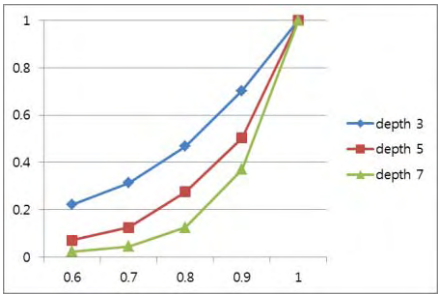
### 5.2 실험결과

그림 4 는 RCA 알고리즘의 성능을 보여준다. x 축은 통합분석시스템의 악성파일분석정확도이다. 그리고 y 축은 공격자를 찾는 비율을 보여준다. 분석정확도가 커질수록 공격자를 찾는 비율이 증가하고 분석정확도가 1 일 때 공격자를 찾는 비율은 100%가 되는 것을 확인할 수 있다. 그리고 공격경로길이 depth 가 길어질수록 공격자를 찾는 비율이 낮아지는 것을 볼 수 있다. 이것은 공격경로길이가 길어질수록 통합분석시스템이 실행파일을 악성이라고 분석하는데 실패하는 확률이 증가하기 때문이다.




(그림 4) RCA 알고리즘의 성능

그림 5 는 HVD 알고리즘의 성능을 보여준다. x 축은 통합분석시스템의 악성파일분석정확도이고 y 축은 총 피해자 노드 중에서 알고리즘의 의해 발견된 피해자 노드의 수의 비율을 나타낸다. 악성파일분석정확도가 증가할수록 숨겨진 피해자 노드의 발견확률이 증가하고 공격경로의 길이가 증가함에 따라 숨겨진 피해자 노드의 발견확률이 낮아지는 것을 확인할 수 있다. 이것은 이전 실험과 같은 이유로 공격경로가 길어질수록 실행파일을 악성이라고 분석하지 못할 확률이 증가하기 때문이다.




(그림 5) HVD 알고리즘의 성능

## 6. 결론

우리는 이 논문을 통하여 네트워크 패킷을 저장하는 사이버 블랙박스 시스템을 소개하고 사이버 공격이 일어났을 때 공격원인을 분석하는 효율적인 RCA 알고리즘을 제안하고 추가적인 중간자나 피해자를 찾는 HVD 알고리즘을 제안하였다. 그리고 시뮬레이션을 통하여 우리의 알고리즘이 효율적임을 보여주었다. 향후 연구에서 우리는 이 알고리즘을 개선하고 실제 테스트 베드에서 사이버 블랙박스 시스템을 사용하여 이 알고리즘의 성능을 테스트할 것이다.

## 참고문헌

[1] Emmanuel S. Pilli, R. C. Joshi and Rajdeep Niyogi, “Network forensic frameworks: Survey and research challenges”, Digital Investigation, 2010

[2] John McHugh, Ron McLeod and Vagishwari Nagaonkar, “Passive Network Forensics: Behavioural Classification of Network Hosts Based on Connection Patterns”, ACM SIGOPS Operating Systems Review, 2008

[3] E. Anderson and M. Arlitt, “Full Packet Capture and Offline Analysis on 1 and 10 Gb/s Networks”, HPL-2006-156

[4] Wei Wang and Thomas E. Daniels, “A Graph Based Approach Toward Network Forensics Analysis”, ACM Transactions on Information and Systems Security, 2008