가상 허니넷 기반 신종공격 탐지 기법

현무용*, 엄익채*, 강대권*
*한전KDN
e-mail:myhyun@kdn.com

Unknown Attack Detection Technique based on Virtual HoneyNet

Mu-Yong Hyun*, Ieck-Chae Euom*, Dae-Kwon Kang*
*KEPCO KDN Co., Ltd.

요 약

최근 정보통신 기술의 발전으로 국가 주요 핵심 기반시설(Critical Infrastructure)의 제어시스템에 대한 개방형 프로토콜 적용 및 외부 시스템과의 연계 등이 점차 증가되고 일반화됨에 따라 국가 핵심 기반시설이 사이버 침해 및 공격에 따른 위협에 노출되고 있다. 특히 기존의 보안기술은 알려진 공격(well-known attack)에만 대응하도록 설계되었기 때문에 공격패턴이 알려지지 않은 신종 공격이 국가 주요 핵심 기반시설을 공격하면 막대한 피해가 불가피하다. 본 논문에서는 최근 IT분야의 화두로 떠오르고 있는 가상화(Virtualization)기술을 적용하여 기존 허니넷 시스템의 장점을 유지하면서 허니넷 시스템의 자원문제, 구축 및 운영관리 문제를 줄일 수 있는 가상 허니넷 모델을 제시하였다. 또한 공격의도 확인기반의 데이터 분석 및 수집기법, 포커스 지향 분석기법을 제시를 통해 분석 결 도출에 필요한 시간비용을 최소화하는 방안을 제안하였다.

1. 서론

정보통신 기술의 발전으로 네트워크 환경이 광역화, 고속화되어 이를 통한 중요 정보의 유출문제가 날로 심각해지고 있다. 현재의 정보통신 기반구조는 서로 밀접하게 연관된 단위 구조들로 구성되어 있어 네트워크 구조의 복잡도 증가로 인한 문제는 더욱 확산되고 있으며, 특히, 국가 주요 핵심 기반시설(Critical Infrastructure)의 제어시스템이 개방형 프로토콜 적용 및 외부 시스템과의 연계 등이 일반화되고 있는 추세이다.[1]

이러한 환경 하에서 침입자의 공격으로 인한 중요 정보의 유출과 제어시스템 자체에 대한 공격은 보안에 대한 심각한 문제점으로 대두되고 있으며, 이를 해결하기 위한 방화벽, 침입탐지시스템, 침입차단시스템 등 다양한 시스템들이 운영 중에 있다.[2]

그러나 상기에 기술된 보안시스템들은 침입자로부터의 공격을 탐지/차단하기 위해 미리 정의된 침입규칙에 의거하여 시스템과 네트워크를 감시하는 기능을 제공하지만 다양한 유형의 공격과 침입규칙에 포함되지 않은 새로운 공격방식에 대한 대처가 불가능하며, 침입대응 시간에서 많은 문제점을 가지고 있다.[3]

허니팟 시스템은 알려지지 않은 공격기법에 효과적으로 대응하기 위해 네트워크상에 침해가 예상되는 컴퓨터를 설치하여 이를 모니터링 함으로써 공격자의 새로운 공격기법이나 공격도구에 대해서 학습하는 시스템이며, 다수의 허니팟으로 구성된 네트워크를 허니넷(Honeynet)이라고 한다.[4]

본 논문에서는 최근 IT분야에서 주목받고 있는 가상화 기술을 응용하여 기존의 고 상호작용 허니팟의 장점을 살리는 동시에 단점을 보완할 수 있는 새로운 가상 허니넷(Virtual Honeynet)의 모델 및 방법을 제시하고자 한다.

2. 허니넷 기반 공격 탐지 방안

2.1 공격의도 기반 데이터 분석기법

2.1.1 호스트 기반 데이터 수집 및 분석기법

Sebekp[4]에서 주요 system call을 가로채어 데이터를 수집하는 방법과는 달리, 서비스 공격의도 확인에 기초한 호스트 기반 데이터 수집 및 분석 기법에서는 TCP, UDP, ICMP에서 각각 66,535개의 포트를 이용하여 서비스를 제공한다는 점에 착안하였다. 즉, 공격자에 의한 악성 코드의 전파행위를 위해서는 사전에 각각의 서비스 제공여부를 스캐닝하게 되는데, 초기 스캐닝에서는 아무런 서비스가 제공되지 않는 것처럼 보이도록 한다.

이후에 같은 포트(서비스)에 대해 추가적인 스캐닝을 하는 경우, 해당 서비스를 제공하고 있는 것처럼 서비스를 시뮬레이션하고, 이후에 공격자나 공격코드의 모든 행위를 수집하는 방식이다. 이러한 방식은 집요하지 않은 공격자를 배제하는 동시에, 공격의도를 가진 공격자나 자동화된 악성코드(예: 웜)의 반복적인 전파행위만을 파악하고 이후에 발생하는 모든 행위를 기록할 수 있다는 장점을 가지게 된다.

2.1.1 네트워크 기반 데이터 수집 및 분석기법

보다 효율적인 데이터 분석 및 결과도출을 위해 본 논문에서는 포커스 지향(Focus-oriented) 분석 기법을 사용하였다. 즉, 호스트 기반 데이터 수집 및 분석부에서 추출한 관심 데이터에 대하여 보다 상세한 분석을 원할 경우, 수집된 네트워크 기반 데이터 풀(Pool)에서 분석하여야 한다.

이러한 경우, 호스트 기반 데이터를 이용하여 네트워크 기반 데이터 풀을 검색할 경우, 추출된 결과 데이터 풀 위에 포커스를 좁혀서 다시 분석할 수 있으며, 이러한 구조는 원하는 분석 결과를 얻을 때까지 반복적으로 수행할

수 있다. 이렇게 함으로써 운영자는 분석 범위를 최소화 할 수 있으므로 보다 효율적으로 원하는 결과에 보다 빨리 도달 할 수 있게 된다.

2.2 공격행위 패턴분류

공격 패턴은 [소스 IP : 목적지 IP : 목적지 포트 : 패킷 길이]로 표현이 가능하다. 예들 들어 *1-1-m-1* 패턴은 외부 고정IP, 내부 고정IP에 가변 내부포트 및 고정길이의 패턴을 의미하며 포트 스캔의 의미를 가진다. 동일한 방법을 적용, 본 논문에서 제시한 서버 허니팟 및 클라이언트 허니팟에 대해 가능한 공격패턴을 분류하면 표1,2와 같다.

<표 1> 서버 허니팟의 공격패턴

공격패턴 종류	패 턴	설 명
포트스캔	*1:1:m:1*	외부의 특정 IP에서 내부의 특정 호스의 여러 포트로 포트 스캔
웜	*1:m:1:1*	외부의 특정 IP에서 내부의 여러 호스트로 특정 포트에 대하여 트래픽이 수렴하는 경우 웜의 패턴
호스트 스캔	*1:m:1:0*	웜의 경우와 유사하나 페이로드가 아주 적은 경우(48바이트 미만)
포트 고정 소스 변조 DoS	*m:1:1:1*	외부의 다양한 IP에서 내부의 특정 호스트/포트로 수렴하는 패턴
분산 호스트 스캔	*m:m:1:1*	외부의 다양한 서버에서 내부의 다양한 호스트로 동일 포트에 대하여 수렴하는 패턴
포트 가변 소스 변조 DoS	*m:1:m:1*	외부의 다양한 호스트에서 내부의 특정 호스트로 다양한 포트의 패턴으로 포트를 가변적으로 변경하며 소스 주소를 위변조하는 공격 패턴
백 스캐터	*1:m:m:1*	외부의 특정 호스트가 내부의 다양한 서버 및 다양한 포트로 공격하는 백스캐터 공격 패턴

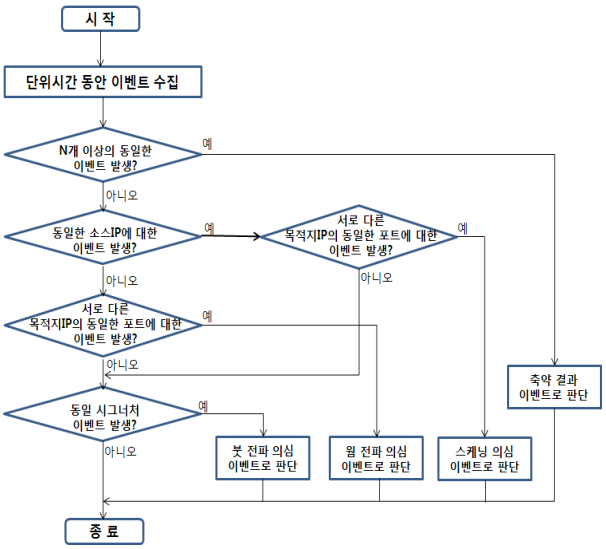
<표 2> 클라이언트 허니팟의 공격패턴

공격 종류	패턴	설명
좀비 공격 (단일 목적지)	*1:1:m:1*	좀비가 된 경우 외부로 단일 공격을 가하는 트래픽 패턴
백 도 어 C&(단일 소스)	*1:m:1:[0/1]*	좀비가 된 경우 단일 숙주 서버로부터 단일 채널의 명령 및 제어를 받는 트래픽 패턴
백 도 어 C&(분산 소스)	*m:1:1:1*	좀비가 된 경우 여러 숙주 서버로부터 단일 채널의 명령 및 제어를 받는 트래픽 패턴
백 도 어 C&(분산 소스)	*m:m:1:1*	좀비가 된 경우 여러 숙주 서버로부터 여러 채널의 명령 및 제어를 받는 트래픽 패턴
좀비공격(분산목적지)	*m:1:m:1*	좀비가 된 경우 외부로 다양한 목적지의 공격을 가하는 트래픽 패턴
DDoS공격	*1:m:m:1*	내부의 좀비가 외부의 특정 호스트로 분산 서비스 거부 공격을 하는 경우 발생하는 패턴

2.3 공격탐지 알고리즘

2.3.1 서버 허니팟 공격탐지 알고리즘

그림 1은 본 논문에서 제안한 서버 허니팟 기반 네트워크 공격탐지 흐름도를 예시하고 있다. 제안된 공격탐지 알고리즘은 패킷수집 모듈에 의해 수집된 패킷 데이터를 기반으로 적어도 하나의 패킷에 대한 소스 네트워크 IP 주소, 목적지 네트워크 IP 주소, 목적지 네트워크 IP의 포트 주소, 패킷크기(Packet size) 및 코드 시그너처 정보에 대한 추출 및 분석이 가능하며, 이를 근거로 허니팟 서버에 대한 공격여부를 판단한다.



(그림 1) 서버 허니팟 공격탐지 프로세스 1

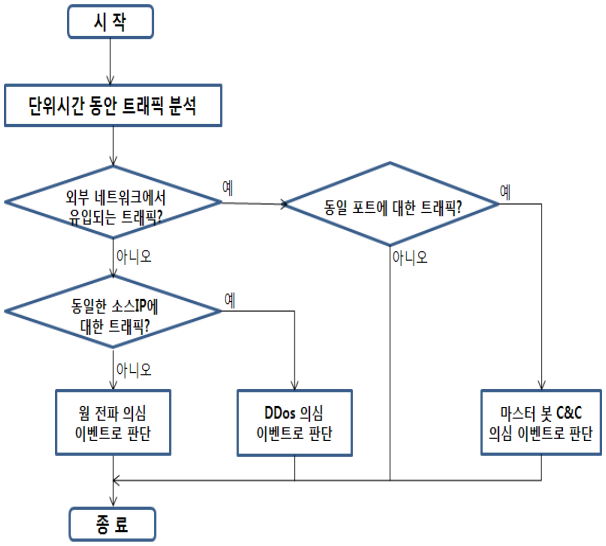
미리 정해진 개수 이상의 동일한 네트워크 이벤트가 발생한 경우에는 축약 결과 이벤트가 발생한 것으로 판단할 수 있다. 한편, 미리 정해진 개수 이상의 동일한 네트워크 이벤트가 발생하지 않은 경우의 분석 흐름은 아래와 같다. 동일 소스 네트워크 IP 주소 및 서로 다른 목적지 네트워크 IP 주소의 동일한 포트 주소에 대한 이벤트가 발생한 경우에는 스캐닝 의심 이벤트로 판단할 수 있다. 서로 다른 소스 네트워크 IP 주소 및 서로 다른 목적지 네트워크 IP 주소의 동일한 포트 주소에 대한 이벤트가 발생한 경우에는 웜 전파 의심 이벤트로 판단할 수 있으며, 동일 코드 시그너처가 식별된 경우에는 봇 전파 의심 이벤트로 판단할 수 있다.

그림 2의 공격탐지 흐름도에 의하면, 소스 네트워크로부터 유입되는 트래픽이 발생하였고 동일 포트에 대한 트래픽인 경우에는 마스터 봇 C&C 의심 이벤트로 판단할 수 있으며, 목적지 네트워크로부터 유출되는 트래픽이 발생하였고 동일한 소스 IP 주소에 대한 트래픽인 경우에는 DDoS 의심 이벤트로 판단할 수 있다. 또한, 목적지 네트워크로부터 유출되는 트래픽이 발생하였고 동일한 소스 IP 주소에 대한 트래픽이 아닌 경우에는 웜 전파 의심 이벤트로 판단할 수 있다.

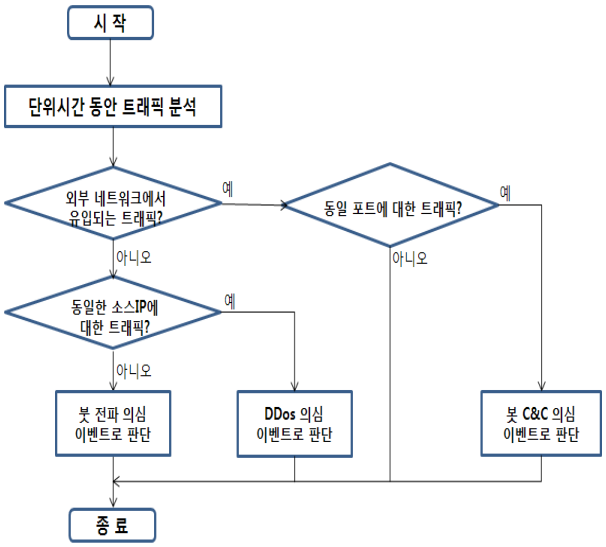
2.3.2 클라이언트 허니팟 공격탐지 알고리즘

클라이언트 허니팟에서는 주어진 단위시간(5분) 동안 클라이언트 허니팟에 들어오거나 나가는 기대되지 않은 트래픽을 분석하며, 탐지프로세스는 그림 3과 같다.

동일한 소스 IP에서 하나 이상의 클라이언트 허니팟의 동일한 포트로 트래픽이 발생할 시는 봇의 C&C



(그림 2) 서버 허니팟 공격탐지 프로세스 2



(그림 3) 클라이언트 허니팟의 공격탐지 프로세스

(Command & Control) 서버로 의심이 되며, 하나 이상의 목적지 IP에서 동일한 소스 IP로 트래픽이 발생할 시는 DDoS가 의심된다. 하나 이상의 목적지 IP에서 다양한 소스 IP로 트래픽이 발생되면 봇 전파가 의심된다.

소스 및 목적지 간의 유입되는 트래픽에 대한 공격탐지 프로세스를 기술하면 아래와 같다. 첫째, TCP/UDP의 64,000개의 모든 포트를 모니터링 및 한 번 이상 동일 포트로 시도하는 공격의도 확인 기반의 공격정보를 수집한다. 둘째, 송신IP-송신포트-수신IP-수신포트의 관계 분석을 통한 Scan, DDoS등의 네트워크 행위 기반 공격 탐지를 한다[3]. 클라이언트 허니팟은 가상머신 상태에서 웹 브라우저를 통해 의심스러운 웹페이지를 직접 실행하는 방식으로 시스템 자원 소모가 크고 분석에 많은 시간이 필요하다. 따라서 제안된 시스템에서는 여러 웹 서버를 동시에 접속하여 악성 사이트를 분석하는 방문 알고리즘을 적용하였다.

여러 웹 브라우저를 통해 웹 서버에 접속 시 클라이언트 허니팟에 비정상적인 상태변화가 발생한 경우, 시스템 후킹을 통해 악성 웹 사이트를 식별하기 위해 해당 웹 서버를 다시 방문한다. 대표적인 방문 알고리즘인 단순 벌크(Simple bulk)알고리즘을 사용하여, 벌크 단위로 웹사이트에 동시 접속 후, 벌크 중에 악성 웹사이트가 있다면 벌크 내의 웹 사이트를 순차적으로 재방문하는 알고리즘을 사용하였다.

2.4 가상 허니넷 시스템

근본적으로 가상 허니넷은 새로운 개념은 아니며 단지 허니넷 기술을 가상화 소프트웨어를 이용하여 한 대의 컴퓨터에 구현하는 개념이다. 이러한 접근 방식은 기존의 허니넷과 비교할 때 고유의 장점과 단점을 가지게 된다. 장점은 명백한 비용절감과 유지 관리가 용이하다는 점이며, 단점은 현재의 가상화 소프트웨어가 Intel X86계열의 하드웨어 시뮬레이션만이 가능하므로 해당 아키텍처를 지원하는 제한된 운영체제만을 지원한다는 점과 공격자가 가상화 소프트웨어를 장악할 경우, 전체 허니넷이 공격자에 의해 장악될 수 있다는 점 그리고 허니넷이 가상화 소프트웨어 위에서 실행되고 있다는 사실을 공격자가 알아낼 수 있다는 점이다.

3. 결론

지금까지 해커의 공격을 탐지하고 차단하기 위해 방화벽, 침입탐지시스템, 침입차단시스템과 같은 많은 보안시스템은 침입자로부터의 공격을 탐지/차단하기 위해 미리 정의된 침입규칙에 의거하여 시스템과 네트워크를 감시하는 기능을 제공하지만 다양한 유형의 공격과 침입규칙에 포함되지 않은 새로운 공격방식에 대한 대처방안이 없으며, 침입대응시간에서 많은 문제점을 가지고 있다.

허니팟은 알려지지 않은 공격이나 악성코드에 의한 네트워크 기반 공격을 탐지하고 분석하는 데 있어 매우 유용한 도구로 사용되어 왔다. 그러나 허니팟의 설치 및 운영에는 많은 물리적 비용과 시간적, 지적 비용이 발생한다.

본 논문에서는 가상화 기술을 이용하여 그동안 문제점으로 제시된 허니팟 구축에 따른 물리적 비용을 최소화할 수 있는 방안을 제시하였고, 공격의도확인 기반의 데이터 분석 수집 및 분석 기법 그리고 Focus-oriented 분석기법을 제시하여 운영에 필요한 비용을 최소화할 수 있는 가상 허니넷의 모델을 제시하였다.

참고문헌

[1] 이명섭, 신경철, 박창현, “거짓세션과 허니팟을 이용한 능동적 침입대응 기법”, 한국통신학회논문지, 30(8C), p.971~984, 2004

[2] More,,S., "A Knowledge-Based Approach to Intrusion Detection Modeling", IEEE SPW 2012, p.75~81, 2012

[3] Yun Yang, "Design and Implementation of Distributed Intrusion Detection System based on Honeypot", ICCET 2010, Vol.6, p.260~263, 2010

[4] Niels P., Thorsten Holz, "Virtual Honeypots from Botnet Tracking to Intrusion Detection", Addison-Wesley, 2007