Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.6.863

Cybertrap : 가상 허니넷 기반 신종공격 탐지시스템

강대권* · 현무용** · 김천석***

Cybertrap : Unknown Attack Detection System based on Virtual Honeynet

Dae-Kwon Kang* · Mu-Yong Hyun** · Chun-Suk Kim***

요 약

최근 정보통신 기술의 발전으로 국가 주요 핵심 기반시설(Critical National Infrastructure)의 제어시스템에 대한 개방형 프로토콜 적용 및 외부 시스템과의 연계 등이 점차 증가되고 있다. 이러한 추세는 국가 핵심 기반시설이 사이버 침해 및 공격에 따른 위협에 노출됨은 물론 사이버 테러 및 해킹, 바이러스 등에 의해 원격 조작 및 통제되는 경우 심각한 위험에 빠질 수 있음을 의미한다. 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(Focus-Oriented) 분석기법을 제시하여 운영비용을 최소화할 수 있는 가상 허니넷 모델을 제안하였다. 제안된 모델을 기반으로 서비스 공격의도 확인 기반의 호스트 및 데이터 수집 기법, 네트워크 공격패턴 시각화 기법 등을 적용한 가상 허니넷 기반의 신종공격 탐지시스템인 Cybertrap을 설계하고 구현하였다. 또한, 제안된 시스템의 시험을 위한 테스트베드를 구축하였고, 일련의 실험을 통해 시스템의 기능 및 성능을 평가하였다.

ABSTRACT

Recently application of open protocols and external network linkage to the national critical infrastructure has been growing with the development of information and communication technologies. This trend could mean that the national critical infrastructure is exposed to cyber attacks and can be seriously jeopardized when it gets remotely operated or controlled by viruses, crackers, or cyber terrorists. In this paper virtual Honeynet model which can reduce installation and operation resource problems of Honeynet system is proposed. It maintains the merits of Honeynet system and adapts the virtualization technology. Also, virtual Honeynet model that can minimize operating cost is proposed with data analysis and collecting technique based on the verification of attack intention and focus-oriented analysis technique. With the proposed model, new type of attack detection system based on virtual Honeynet, that is Cybertrap, is designed and implemented with the host and data collecting technique based on the verification of attack intention and the network attack pattern visualization technique. To test proposed system we establish test-bed and evaluate the functionality and performance through series of experiments.

키워드

Zero-day Attack, Virtual Honeynet, High-Interaction Hoenypot, Client Honeypot, Attack Visualization
제로데이 공격, 가상허니넷, 고상호작용 허니팟, 클라이언트 하니팟, 공격시각화

* 한전KDN(주) 임베디드연구그룹(kang7233@kdn.com) ** 한전KDN(주) SG기반시설보안연구TF(myhyun@kdn.com)
*** 교신저자(corresponding author) : 전남대학교 전자통신공학과(kim1000s@chonnam.ac.kr)
접수일자 : 2013. 04. 15 심사(수정)일자 : 2013. 05. 20 게재확정일자 : 2013. 06. 20

Ⅰ. 서 론

최근 정보통신 기술의 발전으로 네트워크 환경이 광역화, 고속화되어 이를 통한 중요 정보의 유출문제가 날로 심각해지고 있다. 특히 국가 주요 핵심 기반 시설의 제어시스템에 대한 개방형 프로토콜 적용 및 외부 시스템과의 연계 등이 일반화됨에 따라 이러한 환경 하에서 침입자의 공격으로 인한 중요 정보의 유출과 제어시스템 자체에 대한 공격은 보안에 대한 심각한 문제점으로 대두되고 있다[1],[2].

이를 해결하기 위해서 공격 목적에 따른 다양한 보안기술들이 정보시스템 내부에서 불법적인 행동을 감시하고, 추가적인 피해를 막기 위해 방화벽, 침입탐지 시스템, 침입차단시스템 등 다양한 시스템들이 운영중에 있다[3],[4].

그러나 상기에 기술된 침입탐지 및 차단시스템들은 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 내포하고 있다[5],[6].

본 논문에서는 최근 IT분야에서 주목받고 있는 가상화 (Virtualization) 기술을 응용하여 기존의 고 상호작용 허니팟의 장점을 살리는 동시에 단점을 보완할 수 있는 가상 허니넷 기술 기반의 신종공격 탐지 시스템을 설계하고 구현하였다. 또한 일련의 실험을 통해 제안된 시스템의 성능을 평가하고 분석결과를 제시하였다.

Ⅱ. 서비스 공격의도 기반 데이터 수집 및 분석 기법

본 논문에서는 전통적인 데이터 수집 및 분석 기법과 차별화 되는 공격 의도 확인 기반의 데이터 수집 및 분석 기법을 제시함으로써 분석해야할 데이터양을 최소화하고 분석을 최대한 자동화하는 동시에 허니넷의 데이터 수집능력을 극대화하는 기법을 제시하고자 한다.

2.1. 호스트 기반 데이터 수집 및 분석 기법

Sebek[7]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 악성코드의 반복적인 전파행위만을 파악하고 이후에 발생하는 모든 행위를 기록할 수 있다는 장점을 가지게 된다.

2.2. 네트워크 기반 데이터 수집 및 분석 기법

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 도달할 수 있게 된다.

Ⅲ. 공격시각화

3.1. 공격패턴 추출을 위한 핵심 파라미터

이 절에서는 인터넷 공격의 특징들을 규정짓고 분류하기 위한 패킷 헤더정보에 대해 알아보기로 한다. 첫째, 트래픽 정보의 흐름에서 소스 IP, 목적지 IP는 공격자와 희생자 시스템을 의미하는 정보를 나타낸다.

이러한 정보들은 모든 패킷 헤더의 특정 필드에 저장되어 있고, 합법적인 트래픽과 공격트래픽 간의 구분을 위한 정보로 사용가능하다.

둘째, 만약 인터넷 웜의 경우, 일반적으로 TCP 혹은 UDP 프로토콜에서 지정하는 한 개 이상의 포트를 공격목표로 지정하기 때문에 목표시스템의 포트번호를 공격패턴 추출을 위한 핵심 파라미터로 선정할 수 있다.

셋째, 패킷 길이는 해당 트래픽이 정상적인지 비정상적인지에 대한 판단정보를 제공한다. 네트워크 스캐닝과 DoS는 플러딩 프로시쥬어(Flooding Procedure)를 사용하며 해당 공격을 위해 페이로드(Payload)가 없는 공백(Empty) 패킷이 사용되는 것이 일반적이다. 패킷이 페이로드를 가지는 경우라 할지라도 대부분 40 혹은 48 바이트의 고정된 페이로드를 가진다.

인터넷 웜의 경우, 목표 시스템의 취약성의 탐지하기 위한 용도로서 페이로드를 가지며, 대부분의 웜은 일정한 페이로드가 내포되어 전파되기 때문에 웜의 평균 패킷사이즈는 고정된 길이를 가지게 된다. 따라서 패킷 사이즈에 대한 정보를 기반으로 인터넷 웜과 스캐닝 공격에 대한 구분이 가능하다.

3.2. 공격패턴 추출

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 표 1, 2와 같다.

표 1. 서버 허니팟의 공격패턴
Table 1. The attack pattern of server honeypot

공격 패턴 종류	패 턴	설 명
포트 스캔	*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)
포트고정 소스변조 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
포트가변 소스 변조DoS	*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 백 스캐터 공격 패턴

표 2. 클라이언트 허니팟의 공격패턴
Table 2. The attack pattern of client honeypot

공격 종류	패턴	설명
좀비공격 (단일목적지)	*1:1:m:1*	좀비가 된 경우 외부로 단일 공격을 가하는 트래픽 패턴
백도어 C&C (단일 소스)	*1:m:1:[0/1]*	좀비가 된 경우 단일 숙주 서버로부터 단일 채널의 명령 및 제어를 받는 트래픽 패턴
백도어 C&C (분산 소스)	*m:1:1:1*	좀비가 된 경우 여러 숙주 서버로부터 단일 채널의 명령 및 제어를 받는 트래픽 패턴
백도어 C&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

Ⅳ. 가상 허니넷 기반 신종공격 탐지시스템(Cybertrap)의 설계 및 구현

4.1. 시스템의 구성

제안된 시스템은 그림 1과 같이 허니월(Honeywall), VM-허니넷 서버, 허니넷 관리시스템, 포렌식(Forensic) 시스템으로 구성된다. 허니월은 외부로부

터 사설 네트워크 내부로부터 외부로 유출되는 트래픽 중 적어도 하나의 차단 여부를 결정한다. VM-허니넷 서버는 운영체제의 동작을 에뮬레이션 하는 하나 이상의 가상 머신을 포함하며, 네트워크 공격에 대한 데이터를 수집하는 허니팟 역할을 수행한다. 허니넷 관리시스템은 VM-허니넷 서버 운영 관련 가상 머신의 설치, 동작 개시, 동작 중단 및 설정 변경을 제어하며, 허니팟의 동작을 실시간으로 감시한다. 포렌식 시스템은 상기 가상 허니넷으로 유입되거나 가상 허니넷으로 유출되는 패킷 데이터를 수집하는 역할을 담당한다.

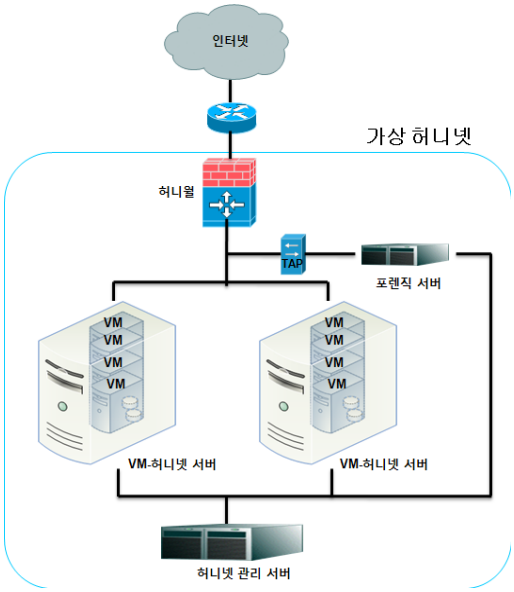


그림 1. 제안된 시스템의 기본 구조
Fig. 1 The basic structure of suggested system

4.2. 공격탐지 알고리즘 설계

4.2.1. 서버 허니팟 기반 공격탐지 알고리즘

그림 2는 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 및 코드 시그너처 정보에 대한 추출 및 분석이 가능하며, 이를 근거로 허니팟 서버에 대한 공격여부를 판단한다.

미리 정해진 개수 이상의 동일한 네트워크 이벤트가 발생한 경우에는 축약결과 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 의

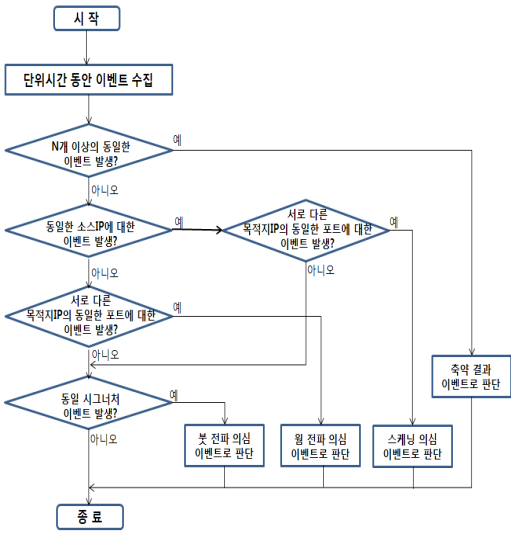


그림 2. 서버 허니팟 공격탐지 프로세스 #1
Fig. 2 Attack detection process of server honeypot #1

심 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 3의 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

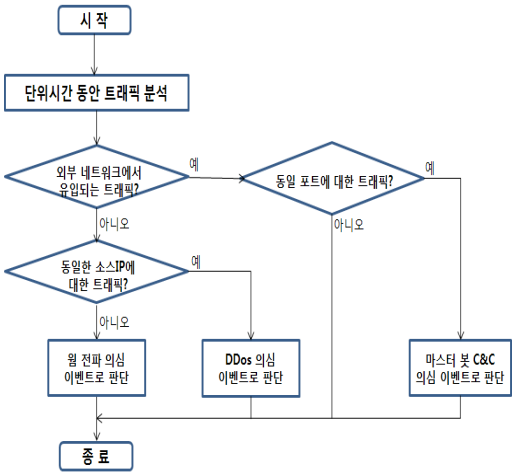


그림 3. 서버 허니팟 공격탐지 프로세스 #2
Fig. 3 Attack detection process of server honeypot #2

아닌 경우에는 웜 전파 의심 이벤트로 판단할 수 있다.

4.2.1. 클라이언트 허니팟 기반 공격탐지 알고리즘

클라이언트 허니팟에서는 주어진 단위시간(5분) 동안 클라이언트 허니팟에 들어오거나 나가는 기대되지 않은 트래픽을 분석하며, 탐지 프로세스는 그림 4와 같다.

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

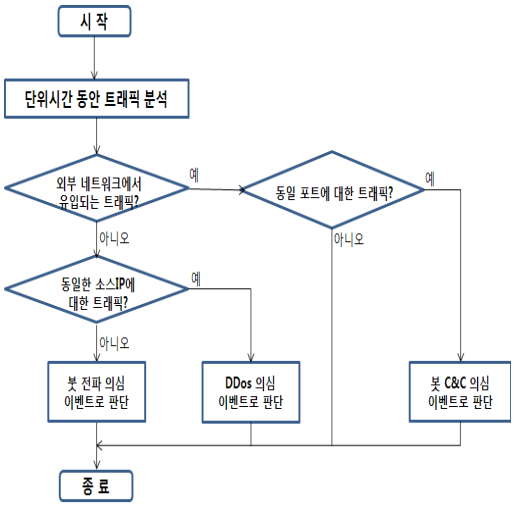


그림 4. 클라이언트 허니팟의 공격탐지 프로세스
Fig. 4 Attack detection process of client honeypot

4.3. 시스템 구현 결과

제안된 시스템은 인텔 CPU 기반의 하드웨어 플랫폼 및 리눅스 운영환경에서 C, AJAX, JSP, Perl 등 다양한 언어로 구현되었다.

제안된 시스템은 허니월, 허니넷 관리시스템, VM-허니넷 서버, 포렌식 시스템으로 구성되며 허니넷 관리시스템에 내장된 클라이언트 프로그램을 통해 설정되고 관리된다. 운영자의 편의를 위해 클라이언트 프로그램은 웹브라우저를 통해 실행가능하며, 윈도우즈, 리눅스 X윈도우, 애블 맥 OS X 플랫폼 환경하의 다양한 웹브라우저를 지원한다. 그림 5는 프로그램 실행 초기화면인 상황판을 예시하고 있다.

상황판은 제안된 시스템이 담당하는 네트워크 자산

에 대한 공격 상황 및 시스템 상황에 대한 정보를 제공한다. 상황판은 지도, 계기판 및 트리 등의 운영자 화면을 통해 표시되므로 사용자가 빠르고 쉽게 상황을 인지할 수 있다. 상황판의 운영자 화면 요소는 크게 전 세계 공격상황 및 시스템 상황으로 구분된다.

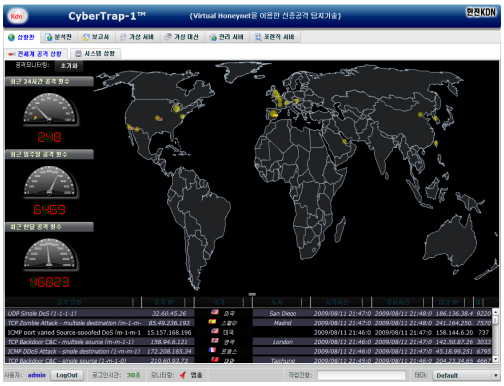


그림 5. 클라이언트 프로그램 실행 초기화면(상황판)
Fig. 5 Initial screen of client program(dashboard)

분석정보 표시기능은 공격정보를 지역별, 유형별로 통계, 지도, 트리맵 등 다양한 방식으로 분석을 지원하는 기능이며, 지역분석, 유형분석의 2가지 분석기능을 지원한다. 그림 6은 제안된 시스템에서 제공하는 지역분석 화면을 보여주고 있다. 분석 작업을 위해 화면 상단의 기간 설정 바에서 데이터의 시작일자와 종료일자를 설정하면 분석 작업을 시작하게 된다. 지역분석은 지도분석, Top 10 공격국가, 레이더 그래프, 공격패턴의 4가지 분석기능을 제공한다.

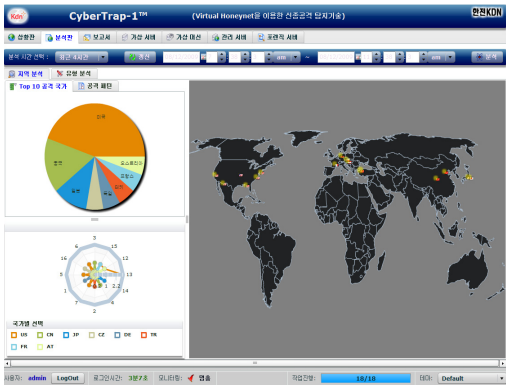


그림 6. 지역분석 화면
Fig. 6 Regional analysis screen

Ⅴ. 실험 및 성능평가

5.1. 실험 환경

그림 7은 본 논문에서 제안한 시스템의 기능 및 성능을 평가하기 위한 테스트베드의 구성을 예시하고 있다.

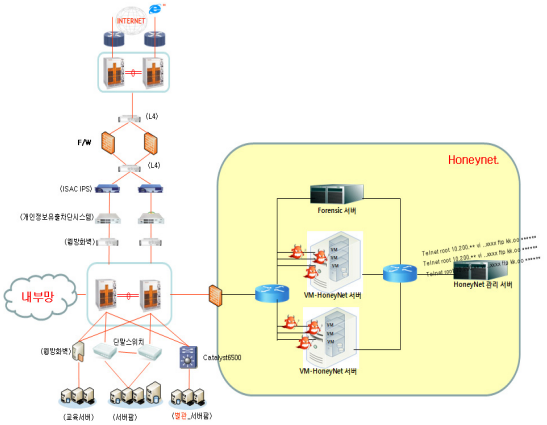


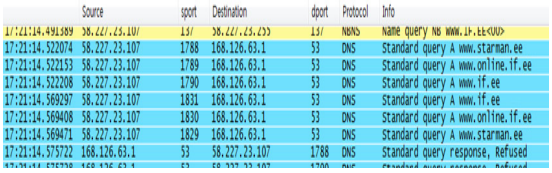
그림 7. 실험 환경
Fig. 7 The experimental environment

테스트베드는 방화벽 내부의 DMZ구간에 설치를 하였다. 방화벽 외부에 설치할 경우에 많은 공격사례를 탐지할 수 있는 장점이 있으나, 제안된 시스템의 하드웨어 제약에 따라 방화벽-IPS 내부에 설치하였다. 이미 알려진 공격에 대해서는 방화벽과 IPS에서 탐지가 가능하기 때문에 테스트베드에서는 현재까지는 알려지지 않은 신종 공격 탐지에 주안점을 두었다.

5.2. 공격탐지 사례 분석

5.2.1 DoS 공격행위 탐지

테스트베드에 본 논문에서 제안한 시스템을 설치한 후 운영한 결과, 그림 8과 같이 가상머신에서 KT DNS로의 트래픽이 짧은 시간 동안 많은 트래픽이 유발되었다. 58.227.23.107 호스트에서 KT DNS로 반복 Query하는 것을 볼 수 있다.



Source	sport	Destination	dport	Protocol	Info
58.227.23.107	137	58.227.23.255	137	NBNS	Name query NB WWW.1F.EE<00>
58.227.23.107	1788	168.126.63.1	53	DNS	Standard query A www.starman.ee
58.227.23.107	1789	168.126.63.1	53	DNS	Standard query A www.online.1f.ee
58.227.23.107	1790	168.126.63.1	53	DNS	Standard query A www.1f.ee
58.227.23.107	1831	168.126.63.1	53	DNS	Standard query A www.1f.ee
58.227.23.107	1830	168.126.63.1	53	DNS	Standard query A www.online.1f.ee
58.227.23.107	1829	168.126.63.1	53	DNS	Standard query A www.starman.ee
168.126.63.1	53	58.227.23.107	1788	DNS	Standard query response, Refused

그림 8. 트래픽 분석 화면
Fig. 8 Traffic analysis screen

제안된 시스템의 상관분석엔진은 이 형태를 “Zombie attack - single destination” 공격으로 탐지하였다. 해당 패킷에 대해 Deep Packet Inspection한 결과 Allaple worm으로 판명이 되었다. Allaple worm은 C&C서버 접속 없이 특정 웹사이트에 대하여 DoS 공격을 하는 Worm으로서 20,80,97,443포트를 이용하여 DoS공격을 수행한다.

하지만 Worm이 KT DNS서버에 특정 웹사이트의 DNS query하였으나 KT DNS서버가 query를 거부함으로서 Allaple worm은 해당 사이트들의 IP주소를 구하지 못하게 되어 실제로는 DoS공격을 수행하지는 못하였다. 이러한 Worm이 국내 일반PC에 대량으로 감염될 경우, KT DNS서버에 부하를 주어 자칫 1.25 대란과 유사한 공격피해를 유발할 수 있다. 추가적인 분석 결과 Allaple worm은 또한 무작위로 ICMP공격을 수행한다.

5.2.1 Port Scan 행위 탐지

외부의 테스트PC에서 허니팟측으로 nmap을 이용하여 Port Scan을 시도하면 제안된 시스템은 "Single-Source-Spoofed DoS[1-1-1-1] worm으로 판단하며, 그림 9와 같이 패턴을 시각화하여 보여준다.

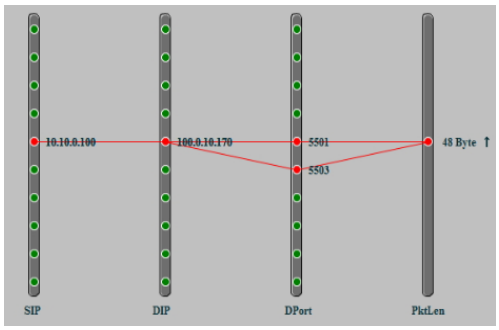


그림 9. Port scan행위 시각화 분석 화면
Fig. 9 Visual analysis screen of port scan

5.2.2 Multi-Get Request 행위 탐지

외부의 테스트PC에서 내부 여러 대의 허니팟 웹서버로 80포트를 이용한 Get방식의 Request행위를 그림 10과 같이 시행하였다. 제안된 시스템에서는 위의 Multi-Get Request 행위를 이상행위로 판단하여 그림 11과 같이 “Packet injected” 이상 행위를 보여주고 있으며 실제 Packet내용도 볼 수가 있다.

```
--- 100.0.10.100 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.244/0.252/0.259/0.008 ms
CMC-MB13:~ mcchae$ ping 100.0.10.168
PING 100.0.10.168 (100.0.10.168): 56 data bytes
64 bytes from 100.0.10.168: icmp_seq=0 ttl=63 time=4.857 ms
64 bytes from 100.0.10.168: icmp_seq=1 ttl=63 time=0.373 ms
^C
--- 100.0.10.168 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.373/2.615/4.857/2.242 ms
CMC-MB13:~ mcchae$ GET http://100.0.10.168
-bash: GET: command not found
CMC-MB13:~ mcchae$ wget http://100.0.10.168
--2011-09-06 12:04:47--  http://100.0.10.168/
Connecting to 100.0.10.168:80... failed: Connection refused.
CMC-MB13:~ mcchae$ wget http://100.0.10.168
--2011-09-06 12:04:51--  http://100.0.10.168/
Connecting to 100.0.10.168:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 30 [text/html]
Saving to: `index.html'

100%[======================================================>]

2011-09-06 12:04:52 (1.30 MB/s) - `index.html' saved [30/30]

CMC-MB13:~ mcchae$ vi index.html
CMC-MB13:~ mcchae$
CMC-MB13:~ mcchae$
CMC-MB13:~ mcchae$
CMC-MB13:~ mcchae$ cat index.html
```

그림 10. Multi-Get Request 실행
Fig. 10 Launched Multi-Get Request

TimeStamp	위...	공격내용	로그	소스IP	목적지IP
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.169
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.169
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.170
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.168
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.170

그림 11. Packet Injected 행위 탐지
Fig. 11 Detection of packet Injected behaviour

Ⅵ. 결 론

차세대 정보전에서는 자신의 정보시스템에 대한 침해방지, 복구 등의 수동적인 행태의 보호뿐만 아니라 상대방의 정보 기반구조에 대한 공격과 같은 적극적인 형태의 보호가 요구된다. 지금까지 해커의 공격을

탐지하고 차단하기 위해 방화벽, 침입탐지시스템, 침입차단시스템과 같은 많은 보안시스템은 미리 정의된 침입규칙에 의거하여 시스템과 네트워크를 감시하는 기능을 제공하지만 침입규칙에 포함되지 않은 새로운 공격방식에 대한 대처방안이 없으며, 침입대응시간에서 많은 문제점을 가지고 있다.

본 논문에서는 가상화 기술을 이용하여 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. 또한, 제안된 모델을 기반으로 신종공격 탐지시스템을 설계하고 구현하였으며, 테스트베드 구축 및 일련의 실험을 통해 제안된 시스템의 기능 및 성능을 평가하였다.

본 논문에서 제시된 가상 허니넷은 공격의 분석 측면에서는 데이터양의 최소화 그리고 분석 비용의 최소화를 달성하였다. 그러나 공격자가 가상 허니넷의 존재여부를 어렵지 않게 파악할 수 있으므로 현재에는 자동화된 악성코드나 초·중급 공격자에 제한적으로 적용될 수밖에 없는 단점을 내포한다. 따라서 가상 허니넷 기술의 사용여부를 은닉할 수 있는 기법에 대한 추가연구가 필요하며, 악성코드 수집 및 분석 기술에 대한 개선이 요구된다.

참고 문헌

[1] Woo-Seok Seo, Jae-Pyo Park, "A Study on Methodology for Standardized Platform Design to Build Network Security Infrastructure", The Journal of The Korea Institute of Electronic Communication Sciences, Vol. 1, No. 1, pp. 203-211, 2012.

[2] Dae-kwon Kang, Ieck-Chae Euom, Chun-Suk Kim, "A Development of Novel Attack Detection Methods using Virtual Honeynet", The Journal of The Korea Institute of Electronic Communication Sciences, Vol. 5, No. 4, pp. 407-411, 2010.

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

[4] Guan Xin, Li Yun-jie, "An New Intrusion Prevention Attack System Model Based on Immune Principle", EBISS 2010, pp. 1~4, 2010.

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

[6] Chun-Suk Kim, Dae-Kwon Kang, Ieck-Chae Euom, "The Case of Novel Attack Detection using Virtual Honeynet", The Journal of Korea Institute of Electronics Communication Science, Vol. 7, No. 2, pp. 279-285, 2012.

[7] MIn-Jae Kim, Hye-Young Chang, "Execution-based System and Its Performance Analysis for Dectecting Malicious Web Pages using High Interactions Client Honeypot", Journal of KIISE (Software and Applications), Vol. 15, No. 12, pp. 1003-1007, 2009.

저자 소개

강대권(Dae-Kwon Kang)

1984년 2월 광운대학교 전자통신공학과 졸업(공학사)
1988년 8월 한양대학교 산업대학원 전자공학과 졸업(공학석사)
2013년 2월 전남대학교 대학원 전자통신공학과 졸업(공학박사)
1995년~현재 한전KDN(주) 임베디드연구그룹장
※ 관심분야 : 정보보호, 전력IT컨설팅

현무용(Muyong-Hyun Hyun)

1992년 경북대학교 컴퓨터공학과 졸업(공학사)
1995년 경북대학교 대학원 컴퓨터공학과 졸업(공학석사)
2003년 충북대학교 대학원 컴퓨터과학과 졸업(공학박사)
1995년~2004년 대원대학교 컴퓨터공학과 조교수
2004년~2005년 일본 산업기술종합연구소 연구원
2005년~현재 한전KDN(주) 선임연구원
※ 관심분야 : 객체기반 분산시스템, 정보보호, PKI기반 인증시스템

김천석(Chun-Suk Kim)

1980년 9월 광운대학교 전자공학과 (공학사)
1982년 9월 건국대학교 대학원 전자공학과(공학석사)
1998년 경남대학교 대학원 전자공학(공학박사)
1982년 11월~현재 전남대학교 전자통신공학과 교수
※ 관심분야 : 수중통신, 정보통신분야