2014년 11월 전자공학회 논문지 제 51권 제 11 호
Journal of The Institute of Electronics and Information Engineers Vol. 51, NO. 11, November 2014 http://dx.doi.org/10.5573/ieie.2014.51.11.127

논문 2014-51-11-16

하이브리드 허니팟 시스템에 대한 연구

(A Study for Hybrid Honeypot Systems)

이 문 구*

(Moon-Goo Lee©)

요 약

다양한 악성코드로부터 정보자산을 보호하기 위해서 허니팟 시스템을 구축한다. 허니팟 시스템은 내부 시스템이 공격받지 않도록 공격을 유인하는 목적으로 설계되거나, 악성코드 정보를 수집하기 위한 목적으로 설계된다. 그러나 기존의 하니팟은 정보 수집을 목적으로 구축되었기 때문에 위장서버 혹은 위장 클라이언트 서버를 구축하거나 위장 콘텐츠를 제공하여 공격자의 유입을 적극적으로 유도하도록 설계되었다. 그러나 위장서버구축의 경우는 빈번한 디스크 입출력으로 약 1년 주기로 하드웨어를 재설치하여야 하고, 위장 클라이언트 서버를 구축하는 경우는 획득한 정보 분석의 자동화에는 한계가 있기 때문에 전문 인력 확보와 같은 운영상의 문제가 있다. 이처럼 기존 허니팟의 하드웨어적인 문제와 운영상의 문제들을 해결 및 보완할 수 있도록 본 연구에서는 하이브리드 허니팟을 제안하였다. 제안한 하이브리드 허니팟은 허니월, 분석서버, 통합콘솔을 두고 공격유형을 2가지 유형으로 분류하여 처리한다. 유형1인 고수준 상호작용서버와 유형2인 저수준 상호작용서버를 동작하도록 하여 위장(유인용)과 거짓응답(에뮬레이션)이 공통스위치 영역에 연계되도록 설계하였다. 이러한 하이브리드 허니팟은 허니월의 저수준 허니팟과 고수준 허니팟을 동작하도록 한다. 분석서버는 해킹유형을 해쉬값으로 변환하고 이를 상관분석 알고리즘으로 분리하여 허니월에 전송한다. 통합모니터링 콘솔은 지속적인 모니터링을 실시하므로 최신 해킹기법과 공격 툴에 대한 정보 분석뿐만 아니라 악성코드에 대한 선제적인 보안대응 효과를 제공할 수 있을 것으로 기대한다.

Abstract

In order to protect information asset from various malicious code, Honeypot system is implemented. Honeypot system is designed to elicit attacks so that internal system is not attacked or it is designed to collect malicious code information. However, existing honeypot system is designed for the purpose of collecting information, so it is designed to induce inflows of attackers positively by establishing disguised server or disguised client server and by providing disguised contents. In case of establishing disguised server, it should reinstall hardware in a cycle of one year because of frequent disk input and output. In case of establishing disguised client server, it has operating problem such as procuring professional labor force because it has a limit to automize the analysis of acquired information. To solve and supplement operating problem and previous problem of honeypot's hardware, this thesis suggested hybrid honeypot. Suggested hybrid honeypot has honeywall, analyzed server and combined console and it processes by categorizing attacking types into two types. It is designed that disguise (inducement) and false response (emulation) are connected to common switch area to operate high level interaction server, which is type 1 and low level interaction server, which is type 2. This hybrid honeypot operates low level honeypot and high level honeypot. Analysis server converts hacking types into hash value and separates it into correlation analysis algorithm and sends it to honeywall. Integrated monitoring console implements continuous monitoring, so it is expected that not only analyzing information about recent hacking method and attacking tool but also it provides effects of anticipative security response.

Keywords: Malicious code, Honeypot, Honeynet, Honeywall, Drive-by-download, Zero-day-attack, correlation analysis, Integrated monitoring consol, Hash value, Attack tool

* 평생회원, 김포대학교 스마트 IT학부 인터넷정보과
(Div. of Smart IT, Dept. of Internet Information, Kimpo College)
© Corresponding Author(E-mail: yeon0330@kimpo.ac.kr)
※ 이 논문은 2014학년도 김포대학교의 연구비 지원에 의하여 연구되었음.
접수일자: 2014년09월03일, 수정일자: 2014년09월30일, 게재확정: 2014년10월30일

Ⅰ. 서 론

최근 악성코드의 감염은 네트워크를 통한 취약한 서비스를 공격하는 방식보다는 사용자가 웹 서핑 중 악의적인 웹 사이트에 접속하는 순간 악성코드에 감염되는 Drive-by-download 방식을 통해 유포되고 있다[1~2]. 이러한 악성코드에 감염된 시스템은 DDoS, 스팸 메일 발송, 개인 정보 탈취와 같은 2차 피해를 유발할 수 있다[3~4]. 본 연구의 구성은 Ⅱ장에서는 허니팟 관련연구로 허니팟의 운영목적과 기대효과, 기존 허니팟의 종류를 소개하고, Ⅲ장에서는 기존 허니팟의 문제점을 보완할 수 있는 하이브리드 허니팟을 구성과 동작방식을 제안하였으며, 마지막으로 Ⅳ장에서는 제안한 하이브리드 허니팟의 장점과 기대효과 등에 대하여 기술하였다.

Ⅱ. 본 론

1. 허니팟의 운영목적과 기대효과

허니팟의 운영목적과 기대 효과 [그림 1]는 해킹행위 즉 웜, 바이러스등과 같은 악성코드를 분석하여 최신 해킹행위에 대한 선제적 대응이 이루어 질 수 있도록 하는 것이 주요 목적이다. 이러한 허니팟의 구축은 내부 인프라 침해여부를 조사하여 내부 침입추론의 기반을 마련할 수 있으며, 아울러 홈페이지 악성코드의 무결성 점검이 이루어질 수 있어야 한다.

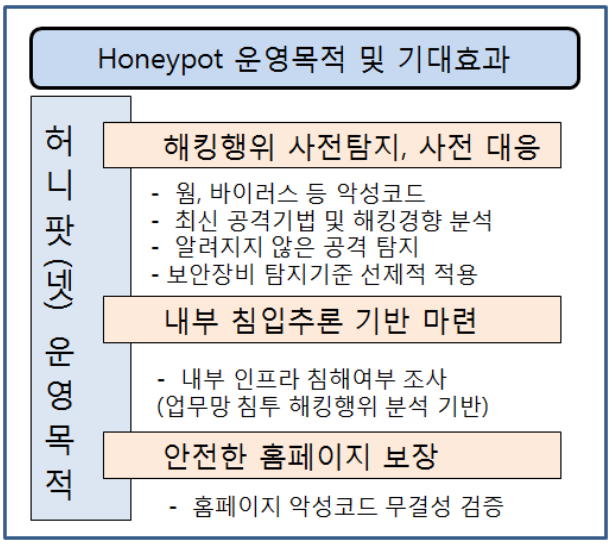

그림 1. 허니팟의 운영목적과 기대효과
Fig. 1. Operation purpose and Expectation Effectiveness of Honey-pot.

2. 허니팟의 종류

허니팟은 크게 두 가지로 구분할 수 있다. 하나는 허니팟 시스템을 이용하여 내부 시스템이 공격받지 않도록 공격을 유인하는 목적의 허니팟 시스템이고, 다른 하나는 유도한 공격의 로그(log : 기록)를 수집하여 향후 공격에 대응할 수 있도록 악성코드 방어기법을 연구하기 위한 정보수집을 목적으로 구성된 허니팟 시스템으로 구분된다[5].

가. 공격 유인 목적의 허니팟

공격 유인목적의 허니팟은 고객사의 웹페이지로 위장하거나 매력적인 위장 콘텐츠를 제공함으로써, 공격자의 유입을 적극적으로 유도하는 방식으로, 해킹과 같은 공격자의 침입을 능동적으로 유도하여 보호해야 되는 정보자산인 내부시스템을 보호하는 목적을 갖는다.

이러한 공격 유인 목적의 허니팟은 쉽게 해커에게 노출되어야하고, 해킹이 가능한 것처럼 취약해 보여야한다. 그렇기 때문에 허니팟 한 대로는 크래커의 유도가 쉽지 않다 따라서, 다수의 허니팟으로 구성된 네트워크 즉, 허니넷(Honeynet)을 구성하는 방법으로 구현된다. 이처럼 공격을 유인하기 위한 목적의 허니팟은 시스템을 통과하는 모든 패킷을 감시할 수 있어야 하며, 관리자는 허니팟 시스템에 접속하는 접속자를 확인할 수 있도록 구성되어야 한다[6]. [그림 2]는 공격유인 목적의 허니팟을 도식화 하였다. 이러한 허니팟은 IP 스캔에 노출되거나, 메인 홈페이지 내 위장 링크를 통해 유인

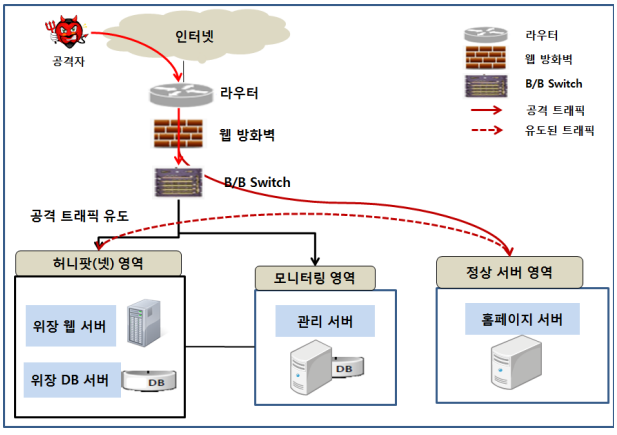

그림 2. 공격유인 목적의 허니팟
Fig. 2. A honeypot of Attack eliciting Purpose.

하거나 웹 방화벽 연동으로 비정상 트래픽일 경유 유도하는 등의 유인 방안을 제공하여야 한다. 그리고 이러한 유인 목적의 허니팟을 구현하기 위해서는 정상서버 영역으로 공격한 트래픽을 허니팟(넷) 영역으로 유도하기 위해 허니팟 영역에 위장 웹서버와 위장 DB서버의 구축과 이를 모니터링영역이 필요하다. 이러한 공격유인목적의 허니팟은 일반적으로 자체 정보 수집력의 강화로 해킹기법 탐지 및 해킹동향 분석 효과를 얻을 수 있으며, 분석결과를 활용하여 보안장비 탐지기준에 대한 선제적 적용 및 시스템 취약점 사전 점검이 가능하도록 구현된다.

나. 정보수집 목적의 허니팟

정보 수집을 목적으로 하는 허니팟의 첫 번째 예로는 위장 서버를 운영하는 방법이다.

이는 위장서버에 설치되어 있는 소프트웨어의 서비스접근, 파일삭제, 위변조 등의 행위에 대한 분석을 수행할 때 알려진 패턴기반의 유해 트래픽을 분석하여 악성코드에 대한 사전 탐지와 선제적 예방대응을 위한 정보를 획득하게 된다[9].

이러한 허니팟은 정보 수집에 목적을 두고 있기 때문에 크래커들을 유인한 후 실제 서비스 네트워크인 것처럼 속이기 위해서는 실제 서비스 네트워크와 격리한 상태에서 실제와 동일한 네트워크 환경을 제공해야 한다. 그러므로 허니팟 한 대로는 크래커의 유도가 쉽지 않으므로 다수의 허니팟으로 구성된 네트워크 즉, 허니넷(Honeynet)을 구성하는 방법이다.

정보수집목적 허니팟의 첫 번째 예는 [그림 3]과 같은 허니팟(넷)으로 표현할 수 있다. 악성코드 정보 수집을 목적으로 하는 허니팟의 다른 사례는 [그림 4]와 같이 위장 클라이언트 서버를 운영하며, 악성의심 SW 수집 및 분석을 위하여 능동적으로 목적 웹페이지를 방문하는 방식이다.

이는 가상머신 환경에서 웹 브라우저를 통해 직접 의심되는 웹 사이트(URL)를 방문하여 클라이언트가 시스템에 허가되지 않은 상태 즉, 파일이나 프로세스 생성, 레지스터리 변경 등의 변화 발생여부를 조사한다.

이처럼 웹사이트에 방문하여 내포된 실행파일과 문서파일을 다운로드하여 실행 및 분석을 수행하기 위해서는 방문 대상인 악성의심 사이트 정보목록인 URL 데이터베이스와 해당사이트를 방문하여 정보를 수집하는

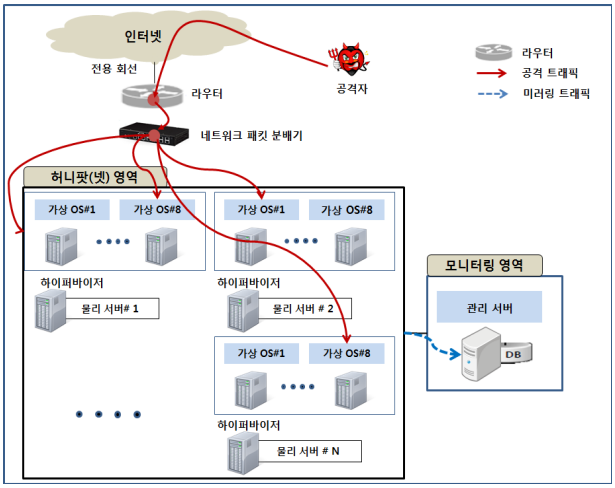

그림 3. 정보수집목적의 허니팟(사례 1)
Fig. 3. A honeypot of information gathering object. (ex. 1)

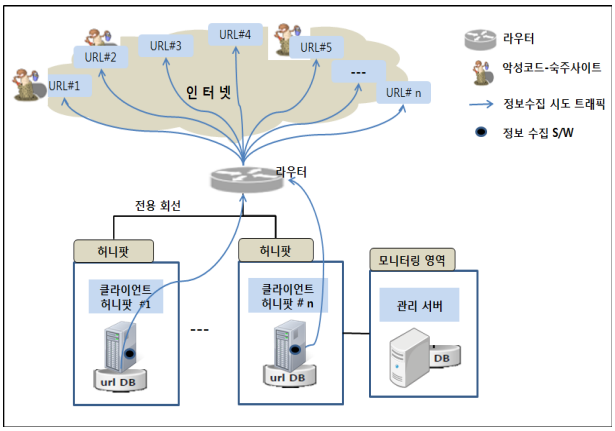

그림 4. 정보수집목적의 허니팟(사례 2)
Fig. 4. A honeypot of information gathering object. (ex. 2)

소프트웨어 그리고 획득한 정보를 분석하는 기술이 필요하다.

Ⅲ. 하이브리드 허니팟

1. 하이브리드 허니팟

기존의 공격 유인을 목적으로 구축된 허니팟의 경우는 정보유인 목적과 함께 시스템의 위험성을 고려하여야 하며, 정보 수집을 목적으로 위장서버를 구축한 허니팟의 경우는 빈번한 디스크의 입출력 발생으로 1년 주기로 하드웨어의 재설치가 불가피한 운영상의 애로사항이 있다. 또한 위장 클라이언트 서버를 두는 경우는 악성 의심사이트(URL)을 대상으로 정보를 분석을 위하

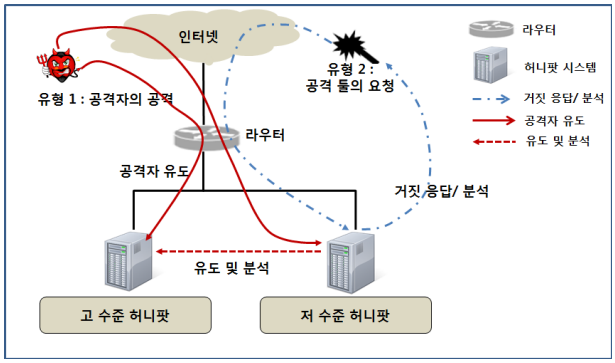

그림 5. 하이브리드 허니팟의 구조
Fig. 5. A structure of hybrid honeypot.

여 자동화하는데 한계가 있으므로 인력부족 등의 운영상의 문제를 갖는다. 이에 본 연구에서는 이러한 문제점들을 최소화하기 위하여 하이브리드 허니팟을 제안한다. 제안하는 하이브리드 허니팟[그림 5]는 고수준 상호작용 허니팟과 저수준 상호작용 허니팟의 2가지 유형으로 분류하여 수행되도록 설계하였다. 유형1은 공격자 해킹행위에 대하여 고수준 실제 서비스 위장 서버가 동작하여 공격자를 유도한 후 악성코드 분석을 수행하고, 유형 2는 공격 툴로부터의 요청에 대하여 거짓응답을 수행(에뮬레이터)하며 공격 툴의 특징을 분석한다.

나. 하이브리드 허니팟 아키텍쳐

하이브리드 허니팟은 정보 수집을 위한 운영체제와 시스템 관리를 위한 운영체제로 분리되어 처리되며, 네트워크도 정보 수집을 위한 네트워크와 관리를 위한 네트워크로 구분되어 설계된다. 하이브리드 허니팟[그림 6]은 공격 트래픽을 유도하여 저수준 상호작용 허니팟과 고수준 상호작용 허니팟에 전송하는 지점에 가상머신(virtual machine)인 허니월(honeywall)을 설계한다.

허니월은 저수준 허니팟에서 고수준 허니팟으로의 공격자 트래픽 재전송을 위한 판단 및 제어를 하며, 공격정보 획득을 위한 공격자 OS 추적, 이상 징후 탐지를 위한 네트워크 흐름 모니터링, 고수준 허니팟의 공격자 악성행위 캡쳐 정보의 수집을 진행한다. 이러한 허니월의 동작을 위해서 분석서버는 외부 데이터를 해쉬함수 알고리즘으로 해쉬값을 산출하여 데이터베이스에 저장하고, 데이터베이스에 저장된 해쉬값은 상관분석 알고리즘에 의해 저수준 및 고수준 상호작용 허니팟에 동작하도록 분류하여 허니월에 전송한다. 통합 모니터링 콘솔은 분석서버의 실시간 분석 결과와 시스템 상태 그리고 실시간 경고를 모니터링 한다.

[그림 7]은 하이브리드 허니팟의 설계를 도식화 한 것이다. 허니월(VM)은 데이터제어(Data Control)모듈과 데이터 캡처(Data Capture)모듈로 구성된다. 데이터제어 모듈은 침입탐지 및 침입방지기능과 저수준 허니팟에서 고수준 허니팟으로의 공격자 트래픽 재전송을 판단하며, 데이터 캡처모듈은 공격정보 획득을 위한 공격자 운영체제 추적, 이상 징후 탐지를 위한 네트워크 흐름 모니터링, 고수준 허니팟의 공격자 악성행위 캡처 정보 수집 등을 수행한다.

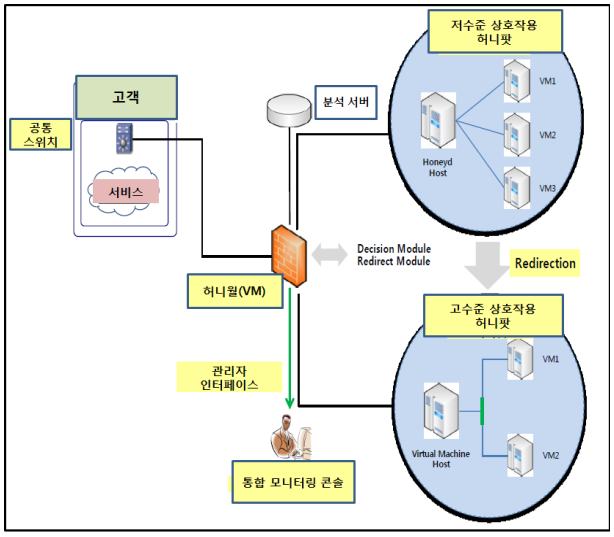

그림 6. 하이브리드 허니팟의 구조
Fig. 6. The Architecture of Hybrid Honeypot.

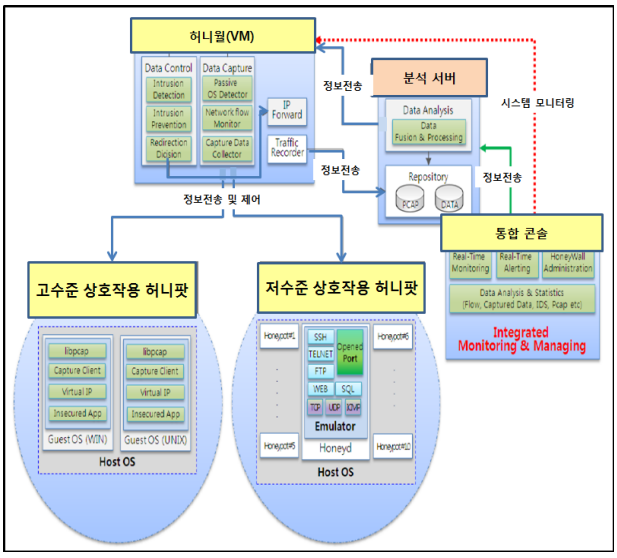

그림 7. 하이브리드 허니팟 설계
Fig. 7. The Design of Hybrid Honeypot.

분석서버의 데이터 분석(Data Analysis)모듈은 저수준 및 고수준, 허니웜의 데이터 정보를 상관분석 처리하여 저장소(repository)에 저장하며, 통합콘솔에 실시간 모니터링/경고/분석/통계 정보를 제공하고, 저장소는 데이터 원본 및 융합분석 결과, 트래픽 덤프를 저장한다. 통합콘솔은 실시간 모니터링(real-time monitoring), 실시간 경고(real-time alerting), 관리(administration) 모듈로 구성된다. 고수준 상호작용 허니팟은 Host/Guest OS, 캡쳐 클라이언트(Capture Client), 불안정한 앱(Insecured App)모듈로 구성하고, 불안정한 앱모듈은 공격자를 유인하기 위해 가상머신(VM)에 설치된 취약한(또는 유인용)서비스기능을 제공한다. 저수준 상호작용 허니팟에서 에뮬레이터(emulator) 모듈은 공격자 요청에 대해 개별 허니팟으로 사전 정의된 스크립트에 의한 거짓 서비스 응답(에뮬레이션)을 수행한다.

2. 하이브리드 허니팟시스템의 동작

제안하는 하이브리드 허니팟은 수집된 악성코드를 효율적으로 저장하고 관리하기 위해서 안전성 및 실용성이 뛰어난 해쉬함수 MD5(Message Digest-5)알고리즘을 사용하도록 제안한다. 수집된 모든 악성코드를 입력값으로 하여, MD5 알고리즘에 따른 16 바이트 해시값을 생성된다. 생성된 악성코드 해쉬값은 분석서버에서 상관분석알고리즘에 의해 유형1과 유형2로 분리되어 처리하도록 설계하였다.

가. 해쉬함수 알고리즘

해쉬 함수 MD5 알고리즘은 가변적 길이의 메시지를 입력값으로 받아들이면 이를 128비트의 해쉬값을 출력시키는 해쉬 알고리즘으로 MD5가 임의의 메시지를 입력으로 받으면 512비트 단위로 처리하며, MD5를 동작시키기 전에 임의의 길이인 메시지를 512비트의 배수가 되도록 채우기(padding)와 마지막 64비트에 원래의 메시지를 2^{64}를 연산한 값 즉 메시지의 하위 64비트 값을

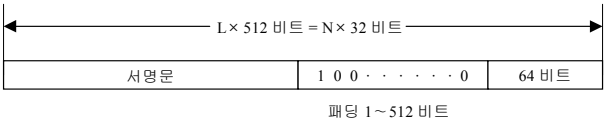

그림 8. MD5의 사전처리과정
Fig. 8. Preprocessing of MD5.

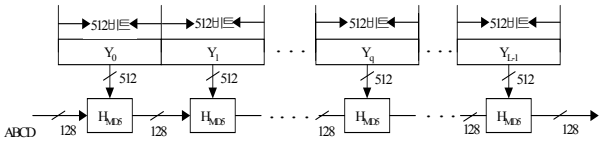

그림 9. MD5의 해쉬연산 흐름도
Fig. 9. Flow Hash Operation of MD5.

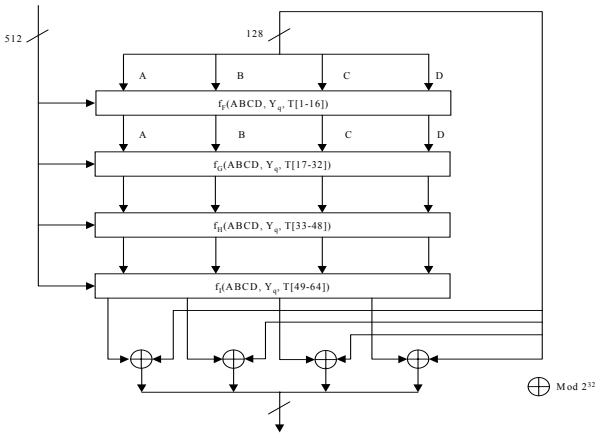

그림 10. HMD5의 처리과정
Fig. 10. Processing of HMD5.

부가하는 사전처리과정(preprocessing)과정 [그림 8]으로 이루어진다[7].

사전처리과정과 해쉬연산을 수행한[그림 9] MD5 알고리즘은 메시지를 512비트씩 16단계(step)로 구성된 4개의 라운드와 4개의 모듈러 덧셈으로 구성된 연산흐름과정 [그림 10]을 수행하여 MD5 해쉬값 HMD5을 얻게 된다. H_{MD5}는 4번의 라운드 처리로 구성된 모듈로서, 각 라운드는 현재의 512비트 블럭 y_a와 128비트 버퍼값 $ABCD$, $T[i]$를 입력으로 처리된다. 이때 $T[i]$는 64개로 각 라운드에 $1/4$씩 입력되며 그 값은 2^{32}x $abs(\sin(i))$의 정수 부분을 의미한다[8].

나. 상관분석

허니웜의 데이터정보(해쉬값)를 상관분석하여 유형1(고수준 상호작용 허니팟)과 유형2(저수준 상호작용 허니팟)로 수행하도록 설계하였다. 해킹공격을 모집단 X라고하고, 공격유형(공격자의 공격 또는 공격툴에 의한 공격)을 모집단을 Y라고 가정하고, 두 변수인 해킹공격(X)과 공격유형(Y)의 상관관계를 기반으로 제안하는 하이브리드 허니팟이 유형1과 유형2로 분리되어 처리되도록 한다. 두 변수의 X, Y축으로 이뤄지는 좌표평면 위에 데이터 점(data point) A와 같이 모든 산점이 두

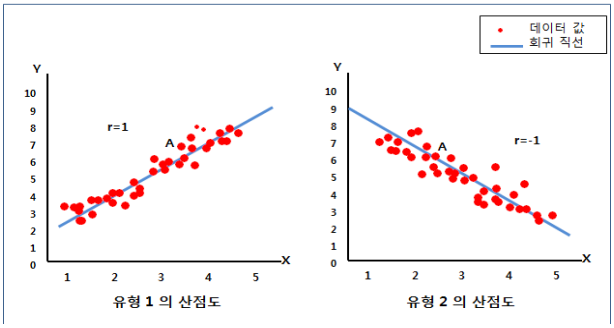

그림 11. 유형1 과 유형 2의 산점도
Fig. 11. Scatter Plot of Type1 and Type 2.

변수 X, Y의 좌표로 표시될 수 있으며, [그림 11]에서 데이터 점 모두를 산점도(Scatter Plot)라 하고, 청색 회귀선을 빼고 산점도로 두 변수 X와 Y의 상관관계를 인지할 수 있다. 데이터 점의 두 변수 X와 Y의 상관관계를 나타내는 피어슨 상관계수(Pearson correlation coefficient)공식을 인용하여 수식 (1)에서 (4)와 같이 정리하였다[9~10].

X 와 Y는 $(X_1, Y_1)(X_2, Y_2),...,(X_n, Y_n)$ 의 모집단이고,
$\overline{X}$, $\overline{Y}$ = X, Y의 평균값 이며,

$$\text{공분산 : } Cov(X,Y) = \sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y}) \quad (1)$$

$$\text{상관계수 } r = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \overline{X})^2 \sum_{i=1}^{n}(Y_i - \overline{Y})^2}} \quad (2)$$

$$r = Corr(X,Y) = \frac{Cov(X,Y)}{\sqrt{Var(X)\,Var(Y)}} \quad (3)$$

$$\text{상관계수 r 은 } -1 \le r \le 1 \text{ 이다.} \quad (4)$$

만약, 모집단 X와 Y가 독립적이라면 $Corr(X,Y) = 0$ 가 되어 상호간의 상관관계는 존재하지 않는다고 할 수 있다[12]. 그러므로 상관계수(r) 값이 1에 가까울수록 공격자 공격유형 X에 근접하므로 공격자의 공격에 대한 고수준 상호작용 허니팟 유형1을 수행하고, -1에 가까울수록 공격 툴에 의한 공격으로 분류되어 저수준 상호작용 허니팟 유형2가 수행된다.

Ⅳ. 결 론

최근 악성코드의 감염은 드라이브 바이 다운로드(Drive-by download)와 같이 보다 치밀하고 사용자가 웹 서핑 중 악의적인 웹 사이트에 접속하는 순간 악성코드에 감염되거나 유포되어 중요한 정보자산의 위협을 받게 되며, 제로데이공격(zero-day-attack)과 같은 공격에 취약하다. 이러한 악성코드로부터 정보자산을 보호하기 위하여 허니팟시스템을 구현하는 여러 가지 방법이 제안되어왔다. 그러나 기존의 위장서버를 구축하는 허니팟시스템의 경우는 빈번한 디스크의 입출력 발생으로 하드웨어의 재설치가 불가피한 운영상의 애로점을 갖으며, 위장 클라이언트 서버를 두는 경우는 악성 의심사이트(URL)를 대상으로 정보를 분석하기 위한 자동화에는 한계가 있으므로 인력부족 등으로 인한 운영상의 문제를 갖는다.

이에 본 연구에서는 이러한 문제점을 최소화하기 위하여 하이브리드 허니팟 시스템을 제안하였다. 제안하는 하이브리드 허니팟은 허니월, 분석서버, 통합콘솔을 허니팟 끝단에 설치하였으며, 허니월은 공격자의 공격과 공격툴에 의한 공격을 분류하며, 저수준 허니팟에서 고수준 허니팟으로의 공격자 트래픽 재전송을 위한 판단과 제어를 한다. 그리고 분석서버는 저수준 및 고수준 허니월의 데이터 정보를 해쉬값으로 저장하고, 이에 대해 상관분석을 적용하여 하이브리드 허니팟의 유형1과 유형2에 따른 동작이 이루어지도록 한다. 통합콘솔은 분석서버의 실시간 분석 결과와 시스템 상태 그리고 실시간 경고를 모니터링 한다. 그러므로 하이브리드 허니팟시스템은 외부로부터의 공격에 대하여 1차적으로 허니월과 분석서버를 통과하므로 기존의 허니팟시스템의 불필요한 장비의 입출력(Device I/O)을 줄일 수 있으며, 공격자의 공격과 공격 툴에 의한 공격에 대하여 유형별로 대응하므로 인력부족으로 인한 운영상의 문제점을 다소 해결할 수 있을 것으로 기대한다. 제안하는 하이브리드 허니팟 시스템은 데이터베이스 자료를 기반으로 내부 침투행위 및 공격 툴 정보를 수집하고 분석할 뿐만 아니라 해킹기법 및 해킹동향과 공격 툴의 정보 분석을 수행할 수 있다. 이러한 정보 활용을 통해 최근의 다양한 해킹공격들에 대하여 선제적인 보안대응 효과를 제공할 수 있도록 설계하였다. 차후에는 설계한 하이브리드 허니팟의 구현과 기존 허니팟시스템과의 성능평가에 대한 연구를 지속하고자 한다.

REFERENCES

[1] M. Cova, C. Kruegel, G. Vigna, “Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code”, IW3C2, Apr. 2010.
[2] M. Egele, P. Wurzinger, C. Kruegel and E. Kirda, “Defending browsers against drive-by downloads: Mitigating heap spraying code injection attacks,” 2009. Available from http://www.iseclab.org/papers/ driveby.pdf; accessed on 15 May. 2010.
[3] B. Endicott-popovsky, J. Narvaez, C. Seifert, D. A. Frincke, L. R. O’Neil, and C. Aval, “Use of deception to improve client honeypot detection of drive-by-download attacks,” Proc. of the 5th Inter-national Conference on Foundations of Augmented Cognition (FAC), 2009.
[4] KrCERT, “Monthly Report: Internet Incident Trends and Analysis”, Mar. 2009.
[5] H. Kim, D. Kim, S. Cho, M. Park, M. Park, “An efficient visitation algorithm to improve the detection speed of high-ineraction client honeypots” RACS 2011, Nev. 2-5, 2011.
[6] C. Seifert, P. Komisarczuk, and I. Welch, “True Positive Cost Curve: A Cost-Based Evaluation Method for High-Interaction Client Honeypots”, SECUREWARE, 2009.
[7] Janaka Deepakumara, Howard Heys and R. Venkatesan, “FPGA Implementation of MD5 Hash Algorithm”, Canadian Conference on Electrical and Computer Engineering, Vol.2, pp.13-16, May. 2001.
[8] Diez J. M., et al., “Hash Algorithm for Cryptographic Protocols: FPGA Implementations”, 10th TELFOR‘ 2002, Nov. 2002.
[9] Hayes, A. F., “Statistical methods for communication science”, 2005
[10] Gravetter, F. J., & Wallnau, L B.“Statistics for the behavioral sciences 8th ed.”, 2008.

저 자 소 개

이 문 구(평생회원)
1984년 숭실대학교 전자계산학 (학사)
1993년 이화여자대학교 대학원 전산교육학 (석사)
2000년 숭실대학교 대학원 컴퓨터시스템 (공학 박사)
2000년 3월～현재 김포대학 스마트 IT학부 인터넷정보과 정교수
<주관심분야 : 알고리즘, 인터넷 보안, 전자상거래 보안, 시스템 보안, 네트워크 보안>