Honeypot과 신경망 IDS를 연동한 진보된 보안 아키텍처 설계

조성환*, 문종섭*

고려 대학교 정보보호 대학원, CIST

Enhanced Defence Architecture Through Combining Honeypot and Neural IDS

Seong-hwan, JO, Jong-sub Moon*

*Center for Information Security Technologies & Graduate School of Information Security
KOREA UNIVERSITY

요 약

최근 증가하고 있는 인터넷 및 기타 네트워크 시스템에 대한 위협은 그 공격의 목적과 기법, 피해의 종류가 늘어남에 따라 효과적인 대응책으로 단순한 기술적 접근 이외에 법률 및 심리, 사회 공학적 접근의 결합적인 대처방안이 강구되어야 할 것이다. 이를 효과적으로 보조할 수 있는 시스템이 Honeypot이다. 하지만 Honeypot 자체는 공격의 위협을 그 즉시 막는데는 별다른 능력이 없기 때문에 Honeypot 시스템의 의도대로 공격자가 속지 않거나 Honeypot의 정보가 다른 보안 도구와 보안 정책 갱신에 이용되기 이전의 공격에 대해서는 취약점을 가지고 있다. 이에 따라 본 논문에서는 기존의 Honeypot 이 설치된 시스템의 효과적 활용을 위해 신경망 이론에 기반한 침입 탐지 모듈을 연동하며 이를 통해 초기 공격에 대한 Honeypot 시스템 보호, Honeypot 시스템이 활성화 된 다음의 상호 연동 효과 및 향후 과제 등을 기술한다. 또한 이에 대한 보다 확실한 접근을 위해 Honeypot 시스템을 통해 DDoS를 방어하도록 제안되었던 시스템의 취약점과 이를 효과적으로 해결할 수 있는 방법을 제안한다.

I. 서론

1. Honeypot 시스템

Honeypot 이란 여타의 일반적인 네트워크 시스템처럼 정상적이며 취약점이 있는 시스템으로 보이도록 공격자를 속여 공격자가 실제 공격을 감행하도록 유도하는 시스템이다. 이러한 침입을 통해 Honeypot은 공격자의 최초 공격시점부터 공격자의 모든 행위를 기록할 수 있으며 공격자의 목표를 분산 혹은 변경시킬 수 있다. 따라서 Honeypot 이 잘 작동하게 되면 일반적으로는 Honeypot 이외의 나머지 네트워크는 보호할 수 있다. 실제 잘 설치된 Honeypot은 공격자에 대한 세부적이고 다양한 정보를 네트워크 보안 관리자에게 제공한다. 이러한 정보의 질적인 향상에 의해 관리자는 기존의 공격 탐지 시스템의 대표적인 문제로 부각되고 있는 False Positive 와 False Negative 문제를 상당 부분 해결할 수 있으며 알려지지 않은 새로운 패턴의 공격에 대해서도 보다 유연하게 대처할 수 있다. 또한 향후 공격자에 대한 증거를 확보, 법적인 대응을 유도하는 Computer forensics, 공격 동기 등에 대한 정보 확보를 통한 심리적 및 사회공학적인 대응 등을 시도할 수 있게 된다. 허니팟은 구현되어지는 레벨에 따라 그리고 설치되어지는 곳에 따라 다양한 목적으로 사용되어 질 수 있다.

2. 신경망 탐지 시스템

신경망은 정상과 공격데이터로 학습데이터를 구성하여 오용탐지와 비정상행위 탐지를 동시에 수행하는 분류를 위한 알고리즘이다. 패턴매칭 시스템의 룰과 비교되는 '학습'이라는 방법을 통해 정상 데이터를 일반화하여, 이에 벗어나는 범주를 탐지하는 비정상행위 탐지와 비정상행위를 일반화하여, 이에 속하는 범주를 탐지하는 오용탐지 모두를 수행할 수 있다.

신경망을 이용한 침입 탐지 시스템은 다음과 같은 장점을 가질 수 있다.

1) 범위의 효율성

환경 변화에 따른 제약 사항에 비교적 강하다는 뜻이다. 신경망은 기존 탐지 시스템에서 행하

여지는 알려진 공격에 대한 룰 설정을 대체할 수 있고 이에 따른 부가적인 정보의 저장이 필요없기 때문이다.

2) 공격에 대한 적응력과 편의성

일반적인 업데이트의 문제를 신경망은 학습을 통한 일반화로 해결한다. 또한 오용탐지와 비정상 행위 탐지 모두를 지원하므로 탐지능력이 뛰어나다.

다만 신경망 시스템의 경우 학습에 필요한 초기 데이터의 질이 상당히 중요하다. 학습을 통해 이뤄지는 일반화는 학습 데이터의 구성에 영향을 많이 받게 된다.

따라서 본 논문에서는 공격이 발생하여 Honeypot에 질 높은 데이터가 저장되어 지면 저장된 데이터를 바탕으로 신경망 탐지 시스템에 갱신을 위해 재사용되어지도록 아키텍처를 설계하였다.

II. 본문

1. 일반적인 Honeypot 운용 형태

일반적으로 Honeypot을 운용할 때에는 크게 2가지를 염두해 두고 운용하게 되는데 첫째는 Honeypot의 동작 레벨을 설정하는 것이고 다른 하나는 Honeypot의 위치를 설정하는 것이다. 두 가지 요소 모두 이 시스템의 가상 공격 주체의 실체에 따라 달라지게 되는데 동작 레벨의 경우 레벨이 높아지면 시스템의 반응도 및 실제 시스템의 유사도가 높아져 공격자를 효과적으로 속이고 유도하는 것이 가능해지는 반면 그만큼 공격에 노출될 가능성이 높아지기 때문에 공격자의 성향과 공격 수준에 따라 가변적으로 운용된다. 또한 설치할 위치는 공격자 외부자인지 내부자인지 공격하고자 하는 부분이 어디인지에 따라 결정된다. 그림 1 에서와 같이 여러 상이한 레벨의 Honeypot 시스템이 동시에 운용되어지는 경우도 많다. 단 모든 Honeypot 시스템은 대부분 공통적으로 해당 네트웍 외부나 격리된 구역에 DB 시스템을 별도로 갖추게 되는데 이는 Honeypot 시스템 자체가 공격을 받게 되는 경우 기록되는 데이터를 신뢰하기 어렵다는 이유에 기인한다.

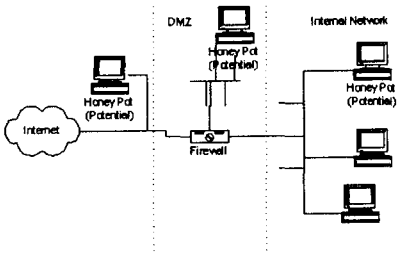

그림 1 일반적인 Honeypot 시스템 운용 예

2.DDoS(Distributed Denial of Service)를 방어하기 위해 고안된 기법 소개

일반적인 DDoS 패턴은 그림 2]와 같이 실명되어 질 수 있다. DDoS 공격은 인터넷의 분산적인 성질을 이용하고 있어서 분산되어 있는 많은 시스템들을 이용해서 대용량의 트래픽을 만들어 낼 수 있다. DDoS 공격을 하기 위해서 공격자는 본격적인 공격전에 많은 공조시스템을 확보해야 하는데,

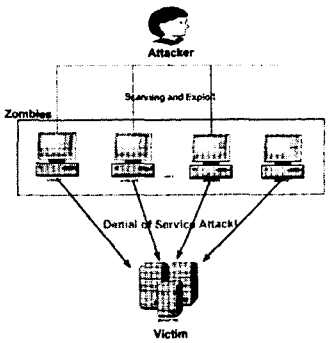

그림 2] DDoS 공격 흐름도

이러한 시스템을 좀비(Zombie)라고 말한다. 이러한 좀비 시스템은 인터넷 여리 군데에 산재해 있으며 자체가 가지고 있는 취약점들을 기반한 공격(Exploit)에 의해 얻어지게 된다. 이렇게 형성된 좀비 시스템들을 조합한 후 특정 명령어나 툴을 사용하여 동시에 같은 명령어를 각 좀비 시스템에 보내게 되고 이에 따라 모든 좀비들은 동시에 이러한 명령을 받고 많은 양의 패킷을 희생 시스템에 보내게 된다. 이러한 기술은 하단에 많은 좀비 시스템들을 이용하기 때문에 공격에 대한 추적 역시 어렵다. 좀비를 찾은 후에 다시 클라이언트를 찾아야 하지만, 클라이언트를 찾더라도 공격자는 이미 다른 곳에서 명령을 내리고 있기 때문에 찾기가 쉽지 않다.

Honeypot 을 이용할 경우 그림2의 좀비에 해당하는 파트를 Honeypot 이 대체한다. 즉, 공격자로 하여금 Honeypot을 좀비로 선택하도록 유도하여 DDoS공격을 진행하도록 하여 전체 네트워크에 상해가 없도록 하는 것이다.[3]

하지만 이를 위해 저자는 3가지 전제 조건을 제시하는데 이는 다음과 같다.

1) 공격은 탐지 가능해야 한다.

2) 공격 패킷은 Honeypot으로 입력된다.

3) Honeypot은 실제 네트워크 인프라스트럭처를 흉내낼 수 있어야 한다.

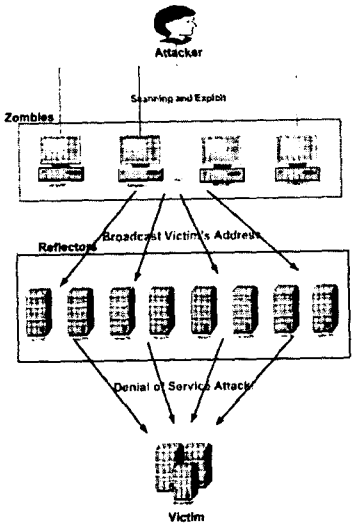

그림 3 DDoS(Reflector사용)

위의 조건들을 언급하기에 앞서 일반적인 공격 절차에 대해 기술해 보자.

그림4을 참조하면 공격은 다음과 같이 이루어지는데 그림에서 공격자가 목표 시스템에 대해 인지하는 과정을 주목할 필요가 있다. 이는 그림에서 보는 바와 같이 DDoS공격에서도 존재한다.

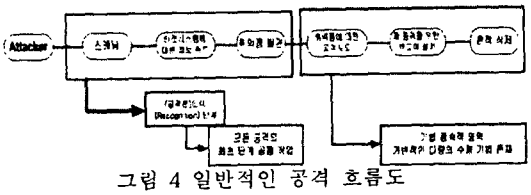

그림 4 일반적인 공격 흐름도

Honeypot 시스템을 이용할 경우 공격자의 잘못된 인지과정(Recognition)유발하여 시스템을 보호하고 공격자에 대한 정보를 획득한다. 따라서 전체 시스템의 성능은 네트워크를 보호하는 목적으로는 탐지 기능에, 공격자에 대한 정보 획득이 목적이라면 공격자를 속이는 기능에 의존한다고 할 수 있겠다.

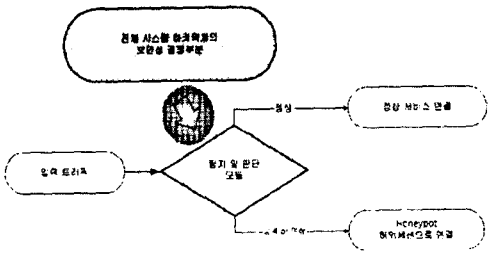

그림 5 DDoS 공격과정 및 인지과정

따라서 [3]의 시스템 역시 위의 두 가지 기능에 전체적인 성능이 좌우되지만 현재 이 기능을 구현하는 과정에서 몇 가지 취약점이 발견된다. 일단 그림6] 은 시스템이 동작하는 원리를 나타낸다.

그림6] 에서는 위의 두 가지 기능 중 공격과 방어의 진행 흐름상 먼저 실행하게 되는 탐지 기능에 대해 강조하고 있다. 시스템은 일단 억세스를 하려고 하는 사용자가 악의적인 이용자인지를 판단하여야 한다. 판단에 성공할 경우 공격자와 정상 이용자의 패킷은 보이기에는 같지만 실제로는 다른 방향의 도착지(정상 이용자는 정상 서비스로, 공격자의 패킷은 Honeypot으로)로 전송되게 된다. 따라서 시스템의 보안성은 판단 모듈의 성능에 좌우되며 특히 지속적인 성능 개선 및 새로운 종류의 공격 기법을 성공적으로 탐지할 수 있어야 한다.

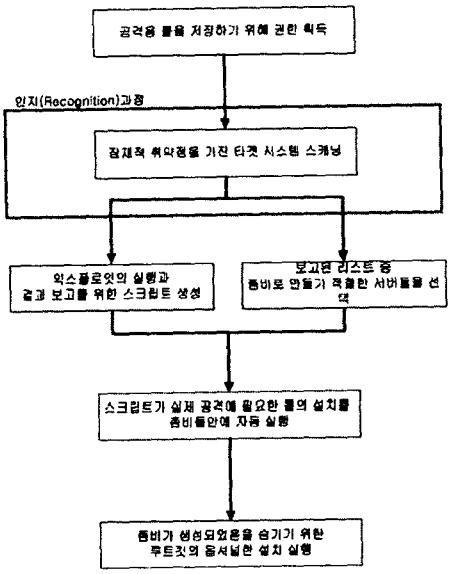

그림 6 Honeypot을 이용한 DDoS 보안 설계

일단 Honeypot으로 연결이 되고 나면 Honeypot은 자신의 시스템으로 들어오는 모든 생산적인 트래픽(Productive Traffic)을 외부의 시스템에 기록(Logging)한다. 이러한 과정은 공격자의 공격 기법뿐만 아니라 공격자의 성향, 동기 및 기타 법적인 절차를 위한 증거 확보에 그 목적이 있기 때문에 Honeypot은 충분한 자료가 확보될 때까지 공격자로부터 정보를 수집하여야 한다. 따라서 Honeypot은 최대한 실제 시스템과 비슷하여야 하며 이를 위해 Honeypot의 인터랙티브 레벨을 높여야 하지만 이는 그만큼의 위험이 따른다.

위의 2가지 부분에 신경망 이론을 이용한 모듈

을 삽입하여 취약점을 제거한 전체 시스템 아키텍처를 설계해보자.

3. 신경망 탐지 모듈과 연동하여 운용

DDoS 공격에 대응하기 위한 기존의 Honeypot 시스템은 위의 3가지 전제 조건을 만족하기 위한 2가지 기능을 구현하는 데 있어 다음과 같은 취약점을 보이게된다.

1) 시스템의 구성 및 의도가 파악될 수 있다.

2) 입력되는 공격패킷을 탐지하지 못할 수 있다.

3) Honeypot 이 공격자의 완전한 통제권 하에 들어간다.

1)은 기술적인 측면에서 볼 때 Honeypot이 효과적으로 공격자를 속이지 못할 때 발생하는 것이다. 2)는 기존의 기법과는 다른 새로운 형태의 공격기법으로 침투가 이루어 질 때 발생하는 것이다. 기존의 탐지 모듈은 정해진 패턴, 시그너쳐(signature) 등을 통해서 부분적인 탐지만이 가능하므로 사실 2)문제가 전체 시스템의 가장 큰 취약성이라 할 수 있다. 3)은 1)의 문제를 막기 위해 Honeypot 시스템의 인터렉티브 레벨을 높였을 때 발생한다. 1), 3) 경우 발생할 수 있는 결과는 공격자의 신속한 회피 같은 것이다. 따라서 공격자에 대한 정보 확보 측면에서는 위와 같은 문제 역시 문제라 할 수 있다. 위와 같은 문제에 효과적으로 대응하기 위해 신경망 이론 기반의 모듈을 설치, 운용한다. 그림7] 은 이를 바탕으로 한 전체 아키텍처이다.

4. 결론 및 향후 연구 과제

단락 2에서 소개한 바와 같이 신경망은 특정한 상황에 대한 학습을 통한 일반화가 강점이다. 즉, 일반 탐지 시스템이 공격에 대한 정보를 DB화 하여 참조하며 탐지하는 방식과 정상적인 시스템 사용에 관한 프로파일이나 상태정보를 이용하여 이것에 벗어난 행위들을 탐지하는 방법을 사용하는 하기 때문에 다양한 특성과 기법을 보유한 공격자의 속성과 분산된 네트워크 환경 하에서의 침입탐지는 익스플로잇되지 않은 그 자체로서도 이미 많은 오류를 발생한다. 대표적인 예가 실제 공격을 탐지하지 못하거나 공격이 아닌데 공격으로 분류하는 false positive 및 false negative 의 문제라 하겠다.

따라서 패턴인식과 분류의 문제를 잘 해결함으로 일반화에 강점을 보이는 신경망 알고리즘을 바탕으로 새로운 공격에 대한 효과적인 탐지 및 이를 통한 시스템의 익스플로잇 방지라 할 수 있겠다. 특히 이 시스템의 익스플로잇의 방지는 전체 네트웍 시스템 및 높은 인터렉티브 레벨로 운용되는 Honeypot 시스템의 익스플로잇을 막는 것 모두를 포함한다. 또한 습득된 데이터를 통해 효과적인 분석작업과 신경망 모듈이 삽입된 각 보안 컴포넌트에 대한 재 학습을 통해 보다 False Negative 및 False Positive의 비율을 줄인 보다 정교한 보안 네트워크를 구축할 수 있다.

시스템을 설치하는 과정에서 실제 침입의 경험이 없거나 너무나 오래된 정보만을 가지고 있을 경우 신경망 알고리즘에 기반한 탐지 모듈은 최소의 데이터를 가지고 최대의 효과를 보여준다. 또한 효과적인 탐지에 뒤이어 허니팟으로 입력, DB화 되어진 질 높은 정보는 분석 후 실시간 및 수동 설정에 의해 탐지 모듈과 Honeypot의 반응 및 레벨 설정을 갱신한다. 따라서 공격 횟수가 증가함에 따라 본 아키텍쳐로 구현된 시스템은 좀 더 높은 공격 탐지율을 보여주며 각 Honeypot에 설치된 신경망 알고리즘을 이용한 호스트 기반 침입 탐지 시스템의 경우 위의 과정을 각 호스트에서 구현함으로써 각 Honeypot이 좀 더 높은 인터렉티브 레벨에서 동작하여 공격자에게 좀 더 실제적으로 반응할 수 있게 하는 기회를 제공한다.

이러한 개선점을 통해 알려지지 않은 공격, 특

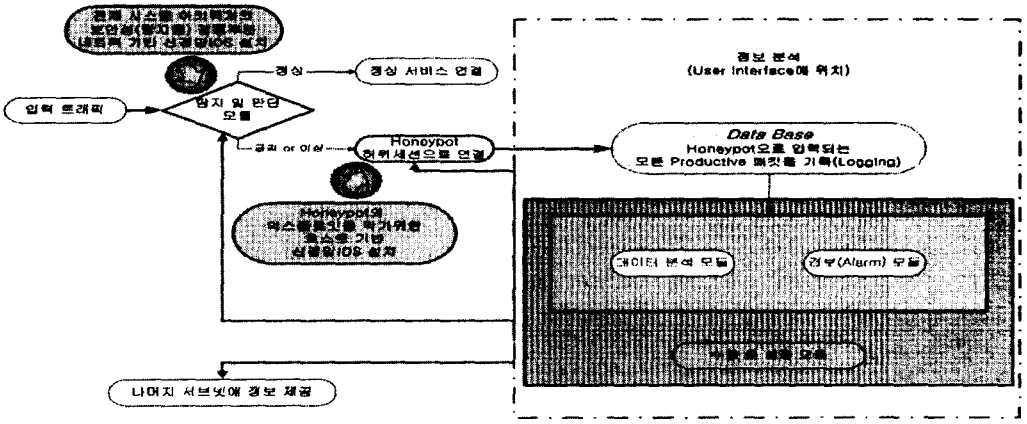

그림 7 신경망 이론과 Honeypot 이 연동된 보안 시스템 아키텍처

히 자동화되고 짧은 시간 안에 동시에 행해지는 새로운 공격법에 효과적으로 대응할 수 있다.

위의 아키텍처는 침입탐지 시스템 및 방화벽, Honeypot 등 다양한 보안 도구를 사용한다. 공격에 대해 접근하고 운용하는 목적에 따라 다양한 운용방법이 예상되므로 이를 효과적으로 관리 할 수 있는 ESM 기법의 연구와 이를 실제로 구현하여 실험할 계획이다. 또한 디지털 면역체계 시스템과 같은 새로운 네트워크 관리 기법을 통해 취약성을 줄이고 공격에 대한 보다 정확하고 다양하게 대응할 수 있는 시스템을 실계할 것이다.

5. 참고문헌

[1] F. Cohen, "A Note on the Role of Deception in information Protection", Computer & Security, Vol 17, 1998, pp. 483-506.

[2] L.Spitzner, " Honeypots - Definitions and Value of Honeypots", Oct 2001,

ttp://www.entercast.com/lspitz/honeypot.html.

[3] Nathalie Weiler, "Honeypots for Distirbuted Denial of Service Attacks," IEEE International WETOCE '02. 2002

[4] Anup K. Ghosh, Aaron Schwatzbard, "A study in using neural network for anormaly and misuse detecion". In Proceedings of the 8th USENIX Security Symposium, August 1999.

[5] Loras R. Even, "What is a Honeypot?: Honey Pot Systems Explained", JUL 12, 2000, http://www.sans.org/newlook/resources/IDFAQ/honeypot3.htm