능동보안 기반구조의 취약점 분석

윤종철*, 강흥식**
*인제대학교 정보컴퓨터공학부
pcman95@hanmail.net
hskang@nice.inje.ac.kr

Assessment of Vulnerability in Active Security Infrastructure

Jong-Chul Yun*, Heung-Seek Kang**
*Dept of Information and Computer Engineering, Inje University

요약

분산시스템의 증가와 인터넷의 확산으로 인하여 네트워크를 통한 공격의 가능성은 점점 커지고 있다. 이러한 잠재적인 위협으로부터 시스템을 보호하기위해 IDS와 Firewall같은 정보보호 시스템들이 개발되었으나, 이들은 네트워크 차원의 효율적인 대응이 어렵고 또한 새로운 공격 패턴이나 보안정책 변화에 적응이 어렵다는 단점을 가지고 있다. 이를 해결하기 위하여 능동보안이라는 분야가 활발히 연구중이나, 능동보안의 기반인 능동 네트워크는 동적이고 유연한 본성으로 인해 그 자체적으로도 심각한 위협을 가지고 있다. 본 논문에서는 능동보안 기반구조의 구성요소와 메커니즘에 대해서 알아보고 능동보안 기반구조에 내포된 취약점을 분석 한다.

1. 서론

컴퓨터 시스템과 네트워크 환경이 발전과 성장을 거듭하여 인터넷을 통한 전자상거래, 홈뱅킹 등의 서비스가 급증함에 따라 네트워크에 대한 침입 피해 사례도 급증하고 있는 추세다. 다수 공격자에 의한 대규모 분산 서비스 거부 공격(DDoS)등 네트워크를 통한 각종 공격이 빈번해짐에 따라, 이러한 위협으로부터 시스템을 보호하기 위해 침입탐지시스템(Intrusion Detection System), 침입차단시스템(Firewall) 등의 정보보호 시스템들이 개발되었다. 이러한 정보보호 시스템들은 침입자에 대한 대응에 중점을 두기 보다는 자신의 도메인을 어떻게 효율적으로 방어 할 것인가에 주안점을 두고 개발되었기 때문에, 해당 침입자의 공격을 탐지하였음에도 불구하고 침입자에 대한 대응이 자신의 도메인에서 그침으로써, 침입자는 제2, 제3의 공격을 할 수 있게 되는 것이다. 또한 새로운 기술을 채택한 공격 방법이 등장하게 되면 이에 대한 탐지 및 대응 기술이 개발되기 전까지는 해당 공격에 대한 아무런 대비책이 없는 상태다. 이에 따라 능동보안이라는 새로운 네트워크 보안 분야가 연구되고 있다. 본 논문의 2장에서는 현재의 네트워크 보안 기술에 대해서 살펴보고, 3장에서는 능동보안 기반구조의 구성요소를 설명하고, 4장에서는 능동보안 기반구조의 메커니즘에 대해서 설명할 것이다. 그 후 5장에서는 능동보안 기반구조의 취약점에 대해서 논의해보고자 한다. 마지막으로 6장에서는 결론 및 향후 방향을 제시한다.

2. 현재 네트워크 보안 기술

현재의 네트워크 보안 기술은 특정 조직이나 특정 도메인을 보호하기 위한 것에 초점이 맞추어져 있으며, 개발되어져 있는 정보보호 시스템은 크게 두 가지로 나뉜다. 침입 징후를 탐지하기위한 침입탐지시스템과 탐지된 해당 침입자의 트래픽을 차단하기위한 침입차단시스템이 그것이다. 초기에는 이 두 시스템이 별도로 운영되었으므로 상호 연동을 위해서는 관리자가 인위적으로 개입하여야 했으나, 현재에는 두 시스템이 표준화된 인터페이스와 API를 정의하는 방법과 이벤트 관리를 이용하여 중앙에서

보안관리를 적용하는 방법 등이 사용되고 있다.

그러나 이러한 통합 보안 역시 관리 대상을 특정 조직이나 특정 로컬 도메인으로 한정함으로써, 침입자에 대한 능동적인 대응이 불가능함으로 새로운 기술을 적용한 제2, 제3의 공격에 취약하다. 현재 적용되는 네트워크 보안 기술은 다음과 같은 근본적인 한계점을 가지고 있다.

a. 침입자는 자유로이 네트워크를 이용할 수 있다. 따라서 동일 시스템에 대한 추가적인 공격이나, 다른 도메인의 다른 시스템에 대한 추가적인 공격이 가능하다.
b. 보안 환경 변화에 대한 적응성이 떨어진다. 보안 정책이 변경되거나 또는 새로운 기술을 적용한 공격에는 무방비 상태다.
c. 동일한 공격에 대해서 전체 네트워크의 다른 부분에서 인식하는 정보와 전체 네트워크에서 수집하는 정보를 상호 결합하는 기능이 부족하고, 또한 서로 다른 도메인끼리의 정보 교환과 상호 협력이 없다.

이러한 한계점을 극복하고자, 침입자의 실제 위치를 추적하고 침입자 근처의 해당 트래픽을 직접 차단함으로써 침입자를 네트워크로부터 단절시키는 연구가 DARPA에서 진행 중이며, 학계를 위주로 기존의 네트워크 기술이나 이동형 에이전트(mobile agent) 기술을 이용하여 침입자를 탐지하기 위한 연구가 진행 중이다.

3. 능동보안 기반구조의 구성요소

능동보안이란 네트워크 침입에 대한 능동적이고 적극적인 대응을 의미한다. [그림 1]에서 보듯이 능동보안 기반구조는 다음과 같은 구성요소들로 구성되어있다.

a. 센서(Sensors)

센서는 보통 네트워크 기반구조의 여러 위치에서 동시에 실행되며 다차원적으로 정보를 수집한다. 센서는 네트워크 공격을 감지하거나 컴퓨터 바이러스를 감지하기 위해 모니터링 하며 이렇게 수집된 정보는 중재자에게 전달된다. 주로 침입탐지 시스템이나 취약점 분석도구, 바이러스 분석도구 등이 여기에 속한다.

b . 중재자(Arbiters)

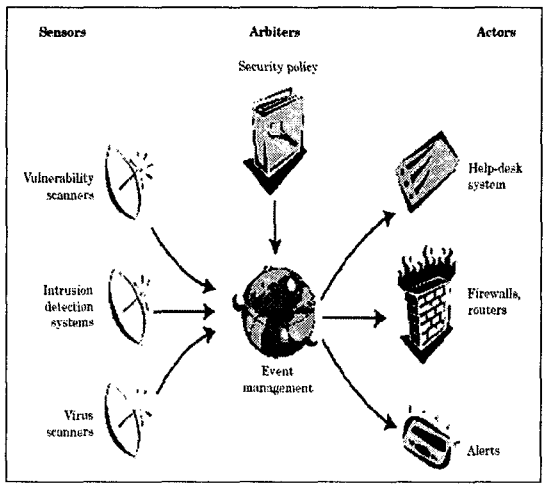
중재자는 센서들로부터 받은 정보를 바탕으로 정책을 결정한다. 중재자의 정책결정은 특별한 보안 정책과 관련이 된다. 특별한 응답/대응이 필요한 경우에는 액터에게 지시한다. 주로 agent라고 불리는 시스템에 탑재된다.

c. 액터(Actors)

액터는 능동보안 기반구조에서 확실한 대응이 필요할 때 그 역할을 하게 된다. 그 뒤에 다른 후속 조치가 필요한지는 그때 상황에 달려있다. 어떤 액터는 단순히 위험을 알리는 장치 일수도 있고 네트워크 중요위치에 놓여져 보안위협을 막기 위해서 동적으로 네트워크에 지시를 가할수도 있다. 주로 help-desk system이나 방화벽 라우터 등이 여기에 속한다.

d. Communication API(통신 프로토콜)

Communication API는 능동보안 기반구조의 구성요소들 사이에 통신을 하기 위한 하나의 가상적인 통신층을 의미한다. 여기서 논하는 통신층의 의미는 OSI 7 Layer에서 응용계층 밑에 하나의 가상적인 통신층을 넣으므로써 각 구성요소간에 신뢰성 있고, 공유가능한 정보를 안전하고 통일된 방식으로 전송하고자 하는데 있다. Commnication API는 PKI(공개키 기반구조)에 그 기초를 두고 있으며, 디지털 인증서(X.509)를 채택함으로써 서로의 정보가 유효한지를 검증 할수 있게 하였다.



[그림 1] Active Security Components

4. 능동보안의 메커니즘

외부로부터 침입을 받았을 경우 아래와 같은 일련의 행동들이 능동보안 기반구조에서 일어난다.

- 제1단계: IDS가 외부로부터의 침입을 탐지
- 제2단계: IDS는 가장 가까운 중재자(Arbiters)에게 침입 사실을 통보
- 제3단계: 중재자는 침입당한 호스트의 라우터에게 해당 트래픽을 차단할 것과 역추적할 것을 지시
- 제4단계: 침해당한 호스트의 라우터는 해당 트래픽을 차단시키고, 인접 라우터에게 해당 트래픽을 라우팅하였는지 묻는다.
- 제5단계: 해당 트래픽을 라우팅시킨 라우터는 라우터에게 물어보는 작업을 반복함으로써 침입을 시도한 호스트와 가장 가까운 최종적인 라우터를 찾아낼 수 있게 됨
- 제6단계: 중재자는 침입자의 라우터에게 침입자의 패킷을 차단시키라고 지시함
- 제7단계: 침입자는 네트워크에서 완전히 차단
- 제8단계: 침해당한 호스트의 복구가 끝나고 침입자의 트래픽이 원천적으로 차단되면, 침해당한 호스트의 라우터의 트래픽 차단을 해지

5. 능동보안 기반구조의 취약점 분석

능동보안 기반구조의 메커니즘을 적용하기위해서는 몇 가지 사항을 고려해야만 한다.

a. 공격자가 목표시스템으로 가기 위해 중간 라우터나 호스트를 경유했을 때 해당 라우터나 호스트는 모든 연결에 대한 감시 기능을 수행하고 있어야 한다. 취약점 분석 장비, 바이러스 탐지 모듈, 침입탐지 모듈과 같은 센서들이 항상 감시를 수행하고 있어야 한다.

b. 네트워크상의 모든 라우팅 장비나 게이트웨이들은 자신들이 라우팅한 패킷에 대한 정보를 남겨야 한다.

c. 모든 네트워크상의 노드들은 Communication API를 내장하고 있어야 하며, 라우팅한 정보를 기록/검색 해야하므로 라우팅 장비의 효율성과 속도가 감소할 수밖에 없다.

d. 능동보안 시스템이 실제로 적용되기 위해서는 communication API가 프로토콜로 구현되어 각 노드들에 탑재가 되어야 하는데, 만약 새로운 기능을 추가하거나 변경하고자 할 때 기존에 장착된 모든 프로토콜을 변경하여야 하므로, 환경변화에 유연하게 대처할 수 없다.

e. 침입자가 동일한 토폴로지 상에 있는 호스트의 IP를 스푸핑하면 역 추적해서 게이트웨이 외부에 있는 라우터에서 차단하더라도, 침입자의 네트워크망의 다른 호스트를 블록 한 것과 같은 결과가 되므로 실효를 거둘 수 없다.

f. 능동보안 기반구조 역시 기존의 IDS를 사용하기 때문에 전혀 새로운 기술을 탑재한 공격에는 속수무책일 수밖에 없으며, 더욱이 중재자 시스템이나 인증을 해주는 CA시스템 혹은 중재자 시스템이 공격을 받게 되면, 해커가 네트워크 망 전체를 통제할 수 있는 권한을 갖게 된다.

이러한 능동보안 기반구조의 태생적 문제점과 여러 가지 문제점 때문에 아직 많은 실험과 연구가 진행되고 있는 실정이다. 역 추적 시스템에 의해 악의적인 공격자를 끝까지 추적하려면 모든 경유지, 즉 전 세계 모든 호스트와 라우터를 능동보안 기반구조에 맞게 바꾸어야 하므로 이는 사실상 불가능하다. 그러므로 능동보안 기반구조는 일부 사설 네트워크 망을 중심으로 구현되어 나가야 할 것이다. 외부로부터의 접속은 방화벽이 차단하고 능동보안 기반구조 내의 컴포넌트들은 내부자의 악의적인 크래킹을 추적하는데 그 초점이 맞춰지고, 약간의 문제점들만 수정이 된다면 능동보안 기반구조는 아주 뛰어난 보안체계를 갖추게 될 것이다.

6. 결론 및 향후방향

능동보안 기술은 현재의 정보보호 시스템이 가지는 문제점을 해결하기 위해서, 보안기본 구조에 유연성을 부여함으로써 새로운 공격 유형에 대한 탐지 및 대응 방법, 그리고 기존 공격 유형에 대한 강력한 대응 방법등을 효율적이고도 시기 적절하게 네트워크와 시스템에 제공할 수 있는 차세대 네트워크 보안 기술이다. 현재 능동보안 기술과 관련하여 표준화가 진행중인 것은 없으며, 학계에서 기존 네트워크 기술을 이용한 이동 에이전트를 이용한 침입의 탐지 및 역 추적에 관한 연구가 진행되고 있는 정도

이다. 특히 미국의 경우 DARPA가 주도적으로 공격자의 추적 및 능동적인 대응을 위한 기술을 개발하고 있으나, 자세한 방향 및 연구 결과에 대한 발표는 미미한 상태이다. 이러한 능동 보안 기술은 연구 초기단계에 있으며, 현실에 적용하는 데에는 해결해야 할 과제가 많이 남아 있는 실태이다. 앞으로 기술적으로나 현실적인 부분에 대한 연구가 진척되고 해결책을 찾는다면, 현재의 네트워크 보안 기술에 비해서 많은 유연성과 확장성을 가지게 됨으로써 보다 능동적이고 신뢰성 있는 보안환경을 제공할 수 있게 될 것으로 보인다.

<참고문헌>

[1]손승원, "Active Security 기술 발전 방향." Sigcomm Review Vol.1, No. 1, Dec. 2000.

[2]이수형 외,"액티브 네트워크 기술 동향" 주간기술동향 제996호, ETRI, May 2001.

[3]안계순, "이동 에이전트를 이용한 네트워크 침입탐지 시스템" 한국정보처리학회 추계 학술발표논문집 제8권 2호 2001.

[4]Dipankar Dasgupta, Hal Brian, "Mobile security agents for network traffic analysis," DARPA Information Survivability Conference & Exposition II, 2001. DiSCEX '01 Proceedings, Volume:2, pp332-340, 2001

[5]Gerhard Eschelbeck, "Active Security - A proactive approach for computer security systems," Journal of Network and Computer Applications(2000) 23, pp109-130