능동 보안 관리 기술에서 센서 무결성 보장을 위한 센서 관리 기술

오승희[0] 이수형 남택용
한국전자통신연구원 정보보호기술연구본부 능동보안기술연구팀
(seunghee5, soohyung, tynam)@etri.re.kr

Sensor Management Mechanism for Sensor Integrity in Active Security Management Technology

SeungHee Oh[O], SooHyung Lee, Taekyong Nam
Electronic and Telecommunications Research Institute,
Information Security Technology Division Active Security Technology Research Team
(seunghee5, soohyung, tynam)@etri.re.kr

요 약

본 논문은 기존의 수동적인 네트워크 보안에서 벗어나 보안 위협에 대해서 능동적으로 대처하고 침입자를 말단에서 블록킹하는 능동 보안 관리 기술에서 센서를 관리하는 기술에 대한 것이다. 여기서 이동 에이전트의 특성인 이동성을 지니고 커널 뿐만 아니라 상위 어플리케이션으로 작동하는 센서를 효율적으로 생성, 이동, 위치 관리 및 소멸하는 방식에 대한 요구사항을 제시한다.

1. 서론

손쉬운 인터넷 사용으로 인해 언제 어디서 누구나 네트워크에 간단하게 연결하여 많은 정보를 주고 받는 시대가 도래하였다. 이에 따라 악의적인 의도로 타인의 정보를 유출하여 악용하는 사건들이 나날이 두드러지게 증가하고 그 수법 또한 다양해지고 있다[1]. 따라서 이제는 보안에 대한 깊은 고려와 더불어 좀더 적극적인 대응이 절실히 필요한 때이다.

따라서 본 논문에서는 지금까지의 수동적이고 자신의 네트워크를 보호하려는데 급급했던 보안에서 벗어나 침입자를 역추적하여 능동적으로 대응하는 능동 보안 관리 기술에 대해서 제안하고, 능동 보안(Active Security) 관리에서 사용하는 센서들을 관리하는 관리 센서(Managing Sensor)의 기능에 대해 알아보고자 한다.

2. 기존의 네트워크 보안 방식

현재까지의 네트워크 보안은 침입차단시스템(Firewall)이나 침입탐지시스템(Intrusion Detection System: IDS) 또는 가상사설망(Virtual Private Network: VPN)을 도입하여, 이것이 설치된 네트워크로 들어오는 트래픽에 대해 사전에 일정 규칙을 정하여 불법적인 침입자(Attacker or Hacker)인지 아닌지 여부를 확인하고, 불법적인 침입자의 경우 트래픽을 차단하여 자신의 네트워크를 보호하는 지엽적이고도 수동적인 방식을 사용하였다.

그러나 이와 같은 방식으로는 분산 환경에서 이루어지는 다수 공격자에 의한 대규모 분산 서비스 거부 공격(Distributed Denial of Service: DDoS)을 예방하기에 한계가 있다. 따라서 기존의 개별적인 보안 시스템을 하나로 연동하여 보다 나은 보안을 제공하기 위한 통합 보안 관리 시스템이 대두되고 있다. 그러나 이기종의 보안 시스템을 하나로 연동하는 데는 역시 많은 문제점이 따르고 있다.

3. 능동 보안 관리 기술 (Active Security Management Technology)

날로 침입자의 침입 방식과 기술이 눈에 띄게 진보하고 있는 현실에서 단순히 자신의 네트워크만을 보호

하고 있는 방식은 미봉책에 불가하다. 따라서 침입자를 역추적(Traceback)하여 추가적인 불법적인 행위를 하지 못하도록 말단에서 고립(Isolation)시키는 적극적이고도 능동적인 대응 방식이 요구된다.

능동 보안 관리 기술이란 앞서 말한 바와 같이 침입자를 역추적하여 고립시킴으로써 네트워크를 보호하는 차세대 보안 관리 방식을 의미한다. 여기서 "능동(Active)"의 의미는 보안 측면에서 네트워크 침입에 대한 능동적인 대응함을 의미하고, 서비스 실행 측면에서는 액티브 네트워크 기술을 이용한 새로운 공격에 대한 탐지 및 대응 기술을 손쉽게 수용하여 이를 동적으로 수행함을 의미한다[2]. 능동적인 대응은 주로 침입자에 대한 역추적과 침입자 트래픽에 대한 대응에 주안점을 갖는 것을 말한다.

능동 보안 관리 기술 적용의 예를 들면, 들어오는 패킷에 대한 정보를 미리 효율적으로 저장해두었다가 침입 사실이 발견된 직후에 저장된 정보에서 침입자에 대한 내용만을 추출하여 센서(Sensor)라는 이동성을 지니고 자체 프로그래밍 능력을 지닌 어플리케이션을 이용하여 역추적하여 침입자가 속한 네트워크에서 직접 블록킹(Blocking)하는 방식이다.

4. 센서 관리 기술

능동 보안 관리 기술에서 침입자를 역추적하고 역추적을 행하기 위해 요구되는 정보를 수집하는 역할을 하는 것이 센서이다.

다시 말해, 센서란 네트워크 침입에 능동적으로 대처하기 위한 소프트웨어 모듈로써, 이동 에이전트의 특성인 이동성을 지니고 있으며 액티브 패킷(Active Packet) 내의 수행 가능한 코드형식으로 전달된다[2]. 센서가 이동 에이전트와 다른 점은 이동 에이전트가 단순히 어플리케이션 코드로 존재하는데 반해 센서는 필요에 따라 커널 뿐만 아니라 상위 어플리케이션으로 작동할 수 있다는 점이다.

센서는 이동 범위에 따라 고정형 센서(Stationary Sensor)와 이동형 센서(Mobile Sensor)로 나눌 수 있으며, 수행위치에 따라서 호스트 센서(Host Sensor)와 네트워크 센서(Network Sensor)로 다시 분류된다. 이동형 센서는 생성되어 소멸될 때까지 여러 노드들 사이를 자유롭게 이동하여 실행되는 센서이고, 고정형 센서는 생성하여 특정 노드로 이동된 후 그 노드에서 소멸할 때까지 상주하는 센서이다. 네트워크 센서는 네트워크 노드 안에서 존재하는 센서이고, 호스트 센서는 호스트에서 존재하는 센서를 의미한다.

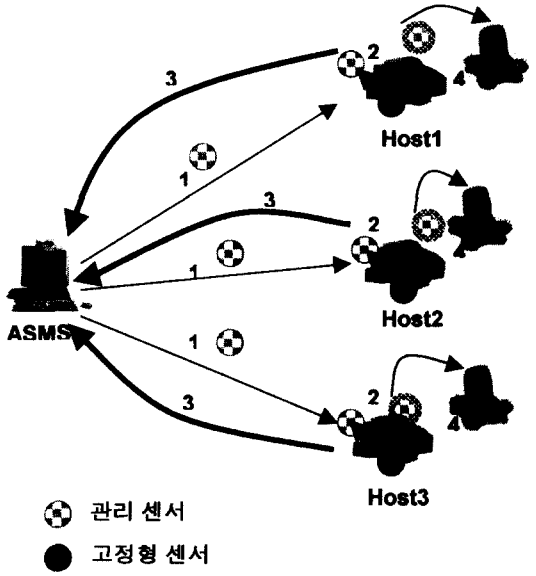
이런 이동형 센서와 고정형 센서 또는 네트워크 센서와 호스트 센서를 관리하는 역할을 하는 것이 관리 센서이다. 관리 센서는 해당 관리 지역내의 노드들 사이를 이동 가능한 이동형 센서로써, 각 도메인 단위로 능동 보안 메커니즘과 보안에 관련된 센서들을 관리하는 서비스를 포함하는 시스템인 ASMS(Active Security Management System)에서 생성하여 임의의 노드로 전송된다. 전송된 관리 센서는 현재 호스트에 상주하고 있는 모든 고정형 센서를 관리하는 역할을 한다.

관리 센서의 주요 역할은 다음의 2 가지로 나누어 볼 수 있다.

- 상주중인 고정형 센서의 작동 여부를 확인
- 임의의 사용자에 의해 고정형 센서가 변경되었는지를 확인하는 무결성 체크

관리 센서가 그 역할을 올바르게 수행하기 위해 요구되는 기능은 다음과 같다.

1. 관리 센서는 이동형 센서로 해당 관리지역 내의 호스트 노드와 네트워크 노드 사이를 자유롭게 이동하며 실행될 수 있어야 한다.
2. 관리 센서는 해당 관리지역 내의 능동보안노드에서 실행 중인 고정형 센서들의 상태(작동 여부)를 주기적으로 체크 할 수 있어야 한다. 이를 위해서 프로세스의 작동 여부를 확인할 수 있는 간단한 명령어를 관리 센서에 코드로 삽입하여 고정형 센서들의 작동 여부를 확인할 수 있다. 이 결과에 대한 분석은 ASMS에서 기존의 값과 비교하여 해당 관리지역 내의 모든 센서들이 작동하고 있는지 알아볼 수 있다.
3. 관리 센서는 해당 관리지역 내의 능동보안노드에서 실행 중인 고정형 센서들의 무결성을 보장해야 한다. 이는 결국 데이터 무결성과 이어진다. 따라서, 자체 침해 여부 확인이 가능한 소스를 관리 센서 안에 코드로 삽입하여 현재 실행 중인 고정형 센서들의 무결성 여부를 확인할 수 있다.



(그림1) 관리 센서의 작동 과정

관리 센서의 생성부터 소멸까지의 모든 작동 과정은 그림 1과 같이 나타낼 수 있고. 이를 다시 단계별로 설명하면 다음과 같다.

1. 해당 ASMS에서 관리 센서를 생성하여 각 호스트로 전송한다.
2. 각 호스트에 도착한 관리 센서가 호스트에 존재하는 고정형 센서와 통신을 통해서 작동 여부와 무결성 체크 한다.
3. 관리 센서는 확인한 고정형 센서의 상태 결과를 ASMS에게 전송한다.
4. 임무를 모두 마친 관리 센서는 자체 소멸한다.

위의 과정은 일정한 시간을 주기적으로 발생하지만, 경우에 따라 비주기적으로 발생하기도 한다. 고정형 센서의 이상이 발견되었을 때 즉시 관리 센서가 고정형 센서가 상주하고 있는 해당 호스트로 전송되는 경우가 바로 비주기적으로 발생되는 한 예이다.

또한 관리 센서가 호스트로 전송되어지면 이를 바로 실행하기 전에 다른 침입자가 전송한 센서가 아닌 자신이 속한 도메인의 ASMS에게서 온 센서라는 사실을 상호 인증을 통해 확인하여야만 한다. 이 때 센서 인증을 위해서는 공개키 방식을 적용할 수 있을 것이며, 센서의 특성상 간단한 코드로 개발된 인증 방식이 사용되어야 할 것이다.

5. 결론

현재의 수동적이고 임시방편적인 침입 대응 방식에서 벗어나 적극적(Aggressive)이고 능동적인 침입 대응 방식이 앞으로 네트워크 보안이 나아가야 할 방향이다

이를 가능하게 해 주는 능동 보안 관리 기술에서는 침입자를 역추적하는데 필요한 정보들과 직접 역추적하는 일련의 과정들을 이동성을 지닌 센서라는 새로운 개념을 이용하여 수행하고 있다. 이러한 센서들을 관리하는 역할을 하는 것이 바로 관리 센서이다. 본 논문에서는 관리 센서의 작동원리와 관리 센서가 지녀야 하는 기능들에 대해서 알아보았다. 관리 센서의 역할 및 기능은 능동 보안 관리 기술의 향후 발전 방향에 따라 변화 가능하다.

앞으로의 연구 계획으로는 이동형 센서와 고정형 센서들간의 통신 및 이들간의 인증 과정에 대한 연구가 지속되어야 할 것이다.

참고문헌

[1] 박정현, "최신 해킹 동향 및 대응 기술", 제7회 정보통신망정보보호 워크숍 발표집, pp 465~478.
[2] "능동보안기술 요구사항 정의서", 기술문서, ETRI, July 2001.
[3] "차세대 인터넷을 위한 능동 보안 기술 백서", ETRI, May 2001.