

네트워크 노드 기반의 이동 에이전트를 이용한 침입탐지시스템에 관한 연구

이기윤, 서대희, 이임영
순천향대학교 정보기술공학부

A study on Intrusion Detection System Using Mobile Agent of Network Node Based

Ki-Yun Lee, Dae-Hee Seo, Im-Yeong Lee
Division of Information Technology Engineering, SoonChunHyang University

요약

최근 인터넷을 대상으로 한 네트워크 공격의 공격 경향은 분산 환경에서 다수 공격자의 대규모 분산 서비스 거부 공격(DoS)의 출현 및 해외 해커들의 국내 전산망을 우회 루트로 활용한 사례의 증가 등 고도화된 불법 행위가 점차 범죄의 강력한 수단으로 이용되는 추세에 있다.

본 논문은 기존 네트워크 노드기반의 침입탐지시스템에서 효율성과 사용자 편의성을 보완하기 위하여 자기 복제가 가능한 이동 에이전트를 적용하여 호스트 간 자율적인 이동을 통해 관리자에게 네트워크 모니터링을 제공하고 침입을 탐지하는 침입탐지시스템을 제안하였다.

1. 서 론

현대인들의 생활은 인터넷 중심으로 그 생활 패턴이 변화되고 있다. 따라서 인터넷이 사회생활의 한 부분을 차지하고 있으며, 또한 인터넷에 접속하기 위한 사용자도 증가하는 추세이다. 따라서 인터넷에 여러 호스트로부터 다량의 개인 프라이버시 정보가 이동하게 되고, 네트워크 공격에 의한 정보유출에는 무방비로 노출되어 있다. 따라서 이러한 침해행위에 대응하기 위한 보안 서비스가 필요하게 되었고 대표적인 보안 서비스인 방화벽(firewall)보다 침입탐지시스템(IDS: Intrusion Detection System)이 최근 각광 받고 있는 보안 서비스이다.[3]

따라서 본 논문에서는 기존의 침입탐지시스템에 대한 방식들을 분석하고 보다 효율적인 침입탐지시스템을 제안하고자 한다. 제안된 방식은 에이전트가 네트워크 상의 호스트들 사이를 자기복제의 개념으로 이동하여 현재 상주해있는 시스템에서 네트워크를 모니터링 하여 침입을 탐지해주는 시스템이다.

2. 기존 침입탐지시스템의 개요 및 분석

다음은 기존의 침입탐지시스템에 개요에 대해 알아보고 이를 분석하고자 한다.

2.1 기존의 침입탐지시스템의 개요 및 필요성

침입탐지시스템이란 실시간으로 탐지하여 대응하는 보안시스템을 의미한다. 침입탐지라는 개념은 1980년 미국의 James P. Anderson에 의하여 최초로 정의되었으며, 그 후로부터 미국에서 지속적으로 연구되어 90년대부터 본격적으로 상용화되었다. 새로운 공격 기법에 대해 방화벽은 대응의 한계를 보게 되었고, 침입에 대해 능동적인 대응을 위해 다수의 시스템에 대한 자동화된 관리와 침입에 대한 전문적인 분석이 가능한 시스템의 필요에 의해서 침입탐지시스템이 사용된다.

2.2 상용화된 침입탐지시스템의 동향

현재 상용화된 침입탐지시스템은 다음과 같은 특징을 가지고 있다.

- 네트워크 기반과 호스트 기반 방식을 모두 채용한 혼합(Hybrid) 방식
- 단일 구조가 아닌 에이전트를 활용한 분산 시스템
- 타 보안시스템과 연동을 통한 대응능력 향상

2.3 기존 침입탐지시스템의 분석

침입탐지시스템은 여러 가지로 분류가 가능하지

만 일반적으로 감사 자료의 자료원에 대해 분류 한다.

2.3.1 호스트기반

호스트 내부에 설치되어 시스템 내부의 상태와 시스템 사용자의 활동을 감시하기 때문에 침입의 성향이나 과정에 대해서 좀더 정확한 탐지가 가능하며, 즉각적인 대응이 가능하다. 그러나 설치와 운영이 까다롭다. 또한 호스트의 시스템 자원을 많이 소모하기 때문에 호스트의 성능저하의 문제를 일으킬 수도 있다.

2.3.2 네트워크 기반

네트워크상의 트래픽을 대상으로 침입을 탐지한다. 따라서 네트워크 상의 모든 호스트들을 관리할 수 있으며, 관리하는 호스트들과는 별도로 설치되어 설치와 운영이 쉽고 호스트 성능과는 무관하게 운영된다. 또한 호스트들 사이에 이루어지는 공격에 대해서 연관관계를 찾아내기 용이하며, 호스트 침입 이전의 공격에 대해서 탐지할 수 있다. 하지만 감시하는 네트워크의 규모에 한계가 있기 때문에 패킷손실로 인한 탐지의 효율성이 떨어지게 된다.

3. 침입탐지시스템의 구성을 위한 보안적 요구사항

일반적인 침입탐지시스템은 다음과 같은 보안 요구사항을 만족해야 한다.[2][9]

① 기밀성

감시의 내용을 관리자나 침입탐지시스템 이외의 시스템이나 사용자가 확인 할 수 없어야 한다.

② 무결성

감시에 필요한 정보나 탐지 결과는 변조되거나 삭제에 대한 보안서비스를 제공해야 한다.

③ 가용성

감시 정보나 탐지 정보가 관리자나 침입탐지시스템이 필요할 때 제공되어야 한다.

4. 이동 에이전트를 활용한 네트워크 노드 기반의 침입탐지시스템 제안

본 논문에서는 이동에이전트를 활용한 호스트 간 자율이동을 통하여 네트워크 트래픽 모니터링 수행하여 침입을 탐지한다.

4.1 시스템 계수

다음은 안전하고 효율적인 침입탐지를 위한 프로토콜의 시스템 계수를 기술한다.

id_A, id_m : 에이전트와 매니저의 식별자

M : 메시지

$E_k()$: 대칭키 알고리즘

K : 대칭키

H() : 안전한 해쉬 함수

L_A : 로그 신호

R_u : 룰 파일

I : 에이전트 실행정보

A, A+1 : 에이전트가 상주해 있는 호스트 주소

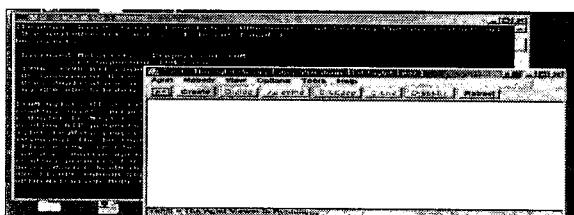
R_h, R_m : 호스트와 매니저에서 생성된 의사난수

4.2 에이전트 운영

에이전트 운영에 대한 프로토콜은 (그림3), (그림5), (그림7)이고 에이전트 생성, 이동, 복제, 폐기의 과정을 통해 에이전트를 운영할 수 있다.

4.2.1 에이전트 생성

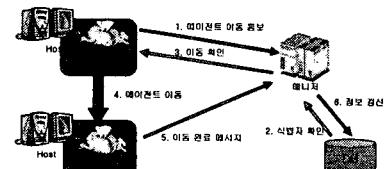
이동 에이전트에서는 별도의 구동환경을 가지며 특정 위치에 관계없이 실행될 수 있는 환경을 제공한다. 구동환경에서는 Class형태로 저장되어 있는 에이전트를 생성하여 활성화 시킬 수 있으며, 생성된 에이전트는 구동환경을 통하여 자유롭게 이동할 수 있다.[1][5]



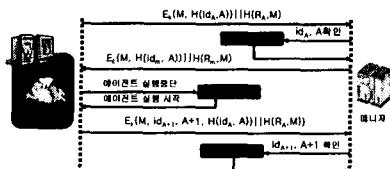
(그림 1) 에이전트의 구동 환경

4.2.2 에이전트 이동 과정

이동 에이전트가 이동은 (그림 2), (그림 3)과 같이 이루어진다.



(그림 2) 에이전트 이동



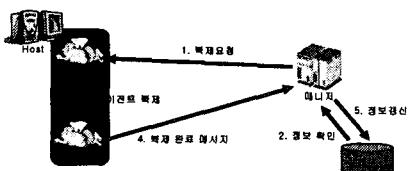
(그림 3) 에이전트 이동에 대한 세부 프로토콜

① 에이전트의 이동은 에이전트 자체에서 자율적으로 수행하며[8], 에이전트는 이동을 매니저에게 통보해준다. 이동할 에이전트의 식별자 id_A 와 대상 호스트의 주소 A를 매니저의 에이전트 데이터베이스에 저장함으로써 에이전트의 위치를 파악할 수 있게 한다.

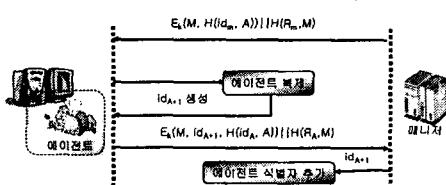
② 매니저는 에이전트의 식별자 id_A 와 호스트 주소 A를 확인한 후에 에이전트 이동을 확인했다는 메시지를 에이전트로 전송 한다. 그리고 에이전트는 이동을 마친 후에 새로운 식별자 id_{A+1} 가 부여되며, 이를 매니저로 전송하여 에이전트 데이터베이스를 갱신하게 된다.

4.2.3 에이전트 복제 과정

이동 에이전트의 복제 과정은 에이전트 개체 조절의 필요에 의해 매니저의 요청에 의하여 수행되며, (그림 4), (그림 5)와 같이 이루어진다.



(그림 4) 에이전트 복제



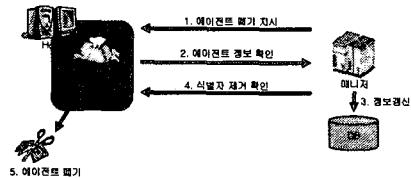
(그림 5) 에이전트 복제에 대한 세부 프로토콜

① 매니저에서 복제 요청 메시지를 에이전트가 받는 즉시 에이전트 복제를 수행하고 복제된 에이전트에는 새로운 식별자 id_{A+1} 가 부여된다.

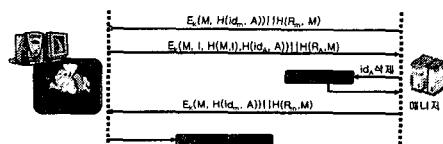
② 복제가 완료된 에이전트는 복제 완료 메시지와 함께 식별자 id_{A+1} 를 매니저에 전송하여 에이전트 데이터베이스에 식별자를 추가한다.

4.2.4 에이전트 폐기 과정

이동 에이전트의 폐기 과정은 에이전트 복제와 마찬가지로 에이전트 개체 조절의 필요에 의해 매니저의 요청에 의해 수행되며, (그림 6), (그림 7)과 같이 이루어진다.



(그림 6) 에이전트 폐기



(그림 7) 에이전트 폐기에 대한 세부 프로토콜

① 매니저에서 폐기 요청 메시지를 받은 에이전트는 에이전트 실행정보 I를 매니저로 전송한다.

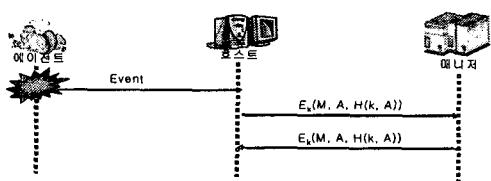
② 매니저는 에이전트 식별자 id_A 를 확인 후에 삭제한 다음 식별자 삭제 메시지를 보내게 된다. 에이전트에서 이 메시지를 전달받으면 에이전트 폐기를 수행한다.

4.3 전체 시스템 운영

에이전트가 매니저와 통신 연결을 수립하고 침입탐지 작업을 수행하는 과정은 (그림 8), (그림 9), (그림 10)과 같이 이루어진다.

4.3.1 연결요구 단계

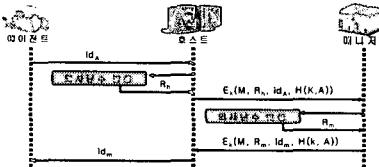
- 에이전트가 매니저와 통신을 하기 위해 연결을 요구하는 과정이다.



(그림 8) 연결 요구 단계 세부 프로토콜

4.3.2 에이전트 인증 단계

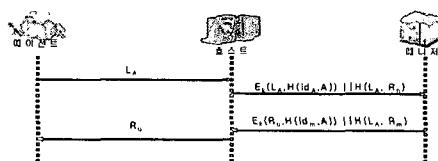
- 에이전트가 정당한 에이전트인지 확인하는 간단한 인증절차이다.



(그림) 9 에이전트 인증 세부 프로토콜

4.3.3 메시지 교환

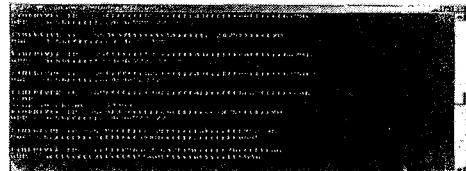
- 에이전트와 매니저 사이에 로그신호나 룰 파일을 전송하는 과정이다.



(그림 10) 메시지 교환에 대한 세부 프로토콜



(그림 11) 룰 파일 적용



(그림 12) 암호화된 템지 로그신호 전송

5. 제안방식 분석

본 논문에서는 기존의 방식보다 효율성을 높이고 편의성을 제공하는 침입탐지시스템을 제안하였다. 침입탐지시스템의 구성을 위한 보안적 요구사항에 부가적으로 다음과 같이 기존 시스템과는 차별화된 특징을 가지고 있다.

① 기밀성

- 에이전트와 매니저사이의 통신은 대칭키 암호 알고리즘으로 암호화하여 공개되지 않도록 보호된다.

② 무결성

- 에이전트와 매니저 사이에 주고받는 메시지는 해쉬 함수를 사용하여 메시지의 내용이 위조 및 변조에 대한 보안서비스를 제공한다.

③ 가용성

- 에이전트의 식별자를 이용하여 정당한 에이전트인지 매니저에서 판별하고, 침입탐지에 대한 정보를 교환 하도록 보안서비스를 제공한다.

④ 효율성

- 에이전트와 매니저사이의 통신은 실시간 침입탐지를 위해 대칭키 알고리즘과 해쉬 함수를 사용하였으며, 에이전트의 개체수를 복제와 폐기의 기능으로 조절할 수 있다.

⑤ 확장성

- 이동에이전트의 활용으로 효과적인 분산시스템을 구축할 수 있으며, 에이전트의 복제로 확장이 용이하다.

⑥ 편이성

- 에이전트의 독립적인 이동으로 에이전트 설치에 따른 부담이 없다.

6. 결론

본 논문에서는 기존의 침입탐지시스템에 대한 방식들을 분석하고 보다 효율적이고 편의성을 제공하는 침입탐지시스템을 제안하였다. 제안된 방식은 이동 에이전트를 활용한 호스트 간 자율이동을 통하여 네트워크 트래픽 모니터링 수행하여 침입을 탐지한다. 그러나 이동 에이전트가 구동할 수 있는 별도의 환경구성이 필요하다는 점이 문제점으로 지적할 수 있다.[1][5]

따라서 본 논문에서 제안되었던 방식을 기반으로 하여 구동환경의 개선에 대한 연구가 지속되어야 한다.

7. 참고 문헌

- [1] 임준식, 황대훈, “이동형 에이전트와 Java 기반의 Aglet 구현기술”, 한국멀티미디어학회지 제3권 제2호 1999년 10월
- [2] 이임영, 이재광, 소우영, 최용락, “컴퓨터 통신 보안”, 도서출판 그린, 2001. 2
- [3] 김재준, “에이전트 기반의 네트워크 침입탐지 시스템”, 순천향대학교, 2002년 11월
- [4] <http://www.certcc.or.kr/>
- [5] Stefano Martino, "A mobile agent approach to Intrusion Detection", Joint Research CentreInstitut for Systems, Informatics and Safety, Italy, June 1999