능동적 해킹 대응 멀티 에이전트 시스템의 설계

하성진°*, 최진우*, 박기형*, 황선태*, 우종우* 고재영**, 정주영**, 최대식**
*국민대학교 컴퓨터학부
**한국전자통신연구소 부설 국가보안기술연구소
e-mail: pcslave@cs.kookmin.ac.kr, dschoi@etri.re.kr

Design of Multi-Agent System for Active Defence from Hacking

Sungjin Ha*, Jinwoo Choi*, Kihyung Park*, Suntae Hwang*, Chongwoo Woo*
Jaeyoung Koh**, Juyoung Jung**, Daesik Choi**
*School of Computer Science, Kookmin University
**National Security Research Institute

요 약

컴퓨터 통신망의 발달로 인해 인터넷은 국가와 사회의 중요한 정보기반으로 자리잡고 있다. 이에 따른 부작용으로 해킹 사고도 단순 과시형에서 범죄적 동기를 갖는 추세로 가고 있으며 이에 대한 대응 또한 능동적이어야 한다는 요구가 제기되고 있다. 본 논문에서는 해킹 사고에 보다 능동적으로 대응할 수 있는 시스템의 설계를 소개한다. 이 시스템은 자율성을 갖고, 시스템의 확장, 변경에 대해 탄력적으로 대처할 수 있게 하기 위해서 멀티 에이전트 시스템으로 구성하였다. 본 논문에서는 상위 레벨에서 해킹 대응 시나리오에 따른 각 에이전트의 활동 및 상호 협력 관계에 대해서 기술한다.

1. 서론[1)]

인터넷이 국가와 사회의 중요정보기반이 됨에 따라 국가 및 사회의 정보기반에 혼란을 주고자하는 범죄적 컴퓨터 침입사건이 점차 증가하고 있다. 인터넷에서 해킹 기술을 이용한 침입자들은 해킹 흔적을 남기지 않고 추적을 피하기 위하여 다른 시스템을 해킹 한 후 목표 서버를 해킹 하는 방식으로 공격을 위한 경유지를 많이 이용하고 있다. 이러한 경유지로 이용된 경우 해커의 추적이 어려울 뿐만 아니라, 최종 피해 기관의 피해 정도가 심각할 경우 공격의 근원지가 아닌 단순히 공격 도중 이용된 경유지이지만 그 책임을 묻는 경우가 발생할 가능성이 존재한다. 지금까지는 중간 경유지를 해킹 한 후 이를 이용하여 해킹 한 침입자를 추적하기 위해서는 경유지로 이용된 기관의 시스템 관리자가 직접 자신의 시스템을 분석한 후 결과를 통보하면 이를 근거로 추적하였다. 이렇게 추적 업무를 각 경유지에서 해당 시스템 관리자의 도움을 받아 시스템을 분석하고 조사하는 과정을 수동 분석에 의존하는 경우 실시간 역추적이 불가능하며, 많은 시간이 소요되기 때문에 수동적인 분석 보다 자동으로 분석할 수 있는 시스템과 공격의 근원지를 추적 가능한 시스템의 필요성이 대두되었다.

이러한 요구에 따라 본 논문에서는 보다 적극적인 방법을 사용한 능동적 해킹 대응 역추적 에이전트 시스템을 제안한다.

이 연구는 ETRI 부설 국가보안기술 연구소 2001년도 위탁연구과제에서 지원 받았음

2. 관련 연구

현재 침입 탐지 기술을 탑재한 다수의 시스템들이 개발되고 있으며 이러한 시스템을 침입탐지 시스템(IDS: Intrusion Detection System)이라 한다. IDS는 모니터링 작업의 대상에 따라 호스트 기반 IDS(host based IDS)와 네트워크 기반 IDS(network based IDS)로 분류된다. 호스트기반 IDS는 하나의 시스템 내부에 시스템 내부 사용자들의 작업 행위를 감시하고 이들의 공격 행위를 탐지해 내는 시스템이며 네트워크 기반 IDS는 네트워크 상의 패킷 캡처링(packet capturing)과 패킷 트레이싱(packet tracing) 기술을 사용하여 이들을 분석, 침입을 탐지해 내는 시스템을 말한다. 이러한 시스템들은 기존의 방화벽(firewall)에서의 수동적 대응과 달리 적극적인 대응 가능한 특징이 있으나 대부분 시스템 관리자에 의존적이며 대응 또한 이들의 경험에 의존해야 한다는 단점이 존재한다. 또한 기존 대부분의 침입 탐지 시스템은 모든 침입 탐지 작업과 이에 상응하는 대응 작업들이 하나의 시스템으로 통합된 단일 시스템 구조이다. 따라서 이런 단일 시스템 구조는 과중한 부하의 유발과 탐지와 대응 모듈의 오동작 및 파괴에 따른 안전성의 문제점을 포함하고 있다

이러한 문제점을 극복하기 위하여 멀티 에이전트 시스템의 개념을 도입하여 내부적인 침입 탐지와 같은 가벼운(lightweight) 작업만을 수행하는 독립적인 자율 에이전

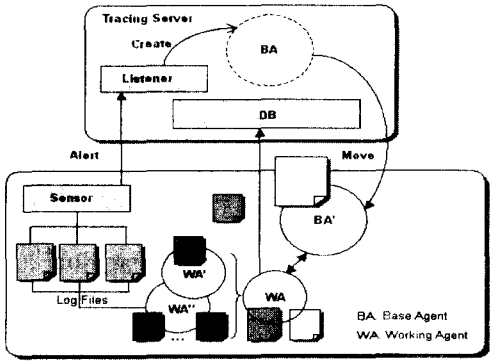
트들(autonomous agents)을 단일 호스트들 상에 탑재하여 모니터링에 따른 시스템의 과중한 부하를 줄이고 여러 시스템들 내의 다른 에이전트들과의 상호 통신을 통한 협력으로 외부의 침입을 탐지, 보고, 대응함으로써 새로운 유형의 침입에 대해 적극적이며 능동적인 대응을 효과적인 수행이 가능하다. 현재 에이전트를 이용한 해킹 대응 시스템에는 대표적으로 IDS[5], AAFID[6] 등이 있으며 기존의 IDS 보다는 분산 환경에서의 수행과 독립적인 에이전트의 기능 면에서 효율적이지만, 역추적 등 능동적 방안을 제시하고 있지는 못하다[7][8].

다중 에이전트 시스템(multi-agent system)에서는 KIF(Knowledge Interchange Format)[1]로 표현되는 에이전트 자신들의 내부 지식을 가지고 또한 공동의 목표를 가지고 에이전트들간의 통신을 경유하여 분산 협동처리에 참여하는 에이전트들을 협력 에이전트(collaborative agent)라 한다. 이들 협력 에이전트들 간의 통신은 정해진 규약에 따른 메시지 패싱(message passing)을 의미하며, 또한 단순한 메시지 패싱 뿐만 아니라 상호 이질적인 에이전트들 간의 통신을 위하여 이해 가능한 프로토콜이 요구되는데 대표적으로 KQML(Knowledge Query and Manipulation Language)[2] 이 활용된다. 이러한 에이전트 기반 기술 언어를 사용함은 에이전트들 간의 지식 통신 전반에 대한 의미 구조를 설계 가능케 하며 보다 효율적인 멀티 에이전트 시스템의 구현이 가능하다[3][4]. 그러나 이러한 에이전트간의 통신 시에 서로 다른 에이전트를 신뢰하고 인증할 수 있는 메커니즘이 요구되는데, 기존의 KQML 프로토콜은 이런 상호 인증을 위한 메커니즘이 포함되어 있지 않기 때문에 에이전트 보호를 위해 KQML상에서의 보안대책이 요구된다. 이러한 KQML 프로토콜의 취약성을 보완하기 위해서 최근에는 KQML의 퍼포머티브 및 매개 변수를 추가하는 연구가 진행되고 있다[9].

본 논문에서는 역추적 등을 통해서 해킹에 보다 능동적으로 대처할 수 있는 시스템을 설계한다. 시스템의 경량화 및 적응성을 갖기 위해서 멀티 에이전트 시스템을 도입하며 상위 레벨에서 에이전트의 활동 및 협력에 관한 시나리오를 중심으로 기술한다.

3. 역추적 에이전트 시스템의 설계

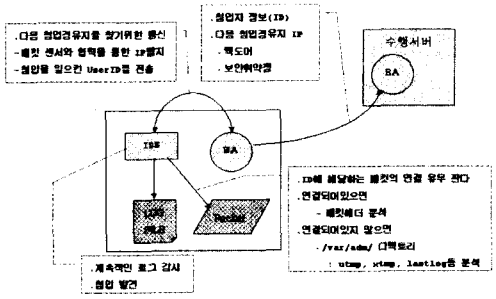
역추적 에이전트 시스템의 구성은 수행 서버와 에이전트들로 구분된다[그림 1]. 수행 서버의 대표적인 기능은 에이전트를 공격의 경유지 또는 공격의 근원지로의 파견을 담당하며 가장 먼저 파견되는 에이전트를 기지 에이전트(Base agent: BA)라 명명하였다. 기지 에이전트는 또한 역 추적을 위한 정보를 수집하기 위해 여러 작업 에이전트(Working Agent: WA)들을 생성한다. 역추적 에이전트 시스템의 기능은 크게 공격을 위한 중간 경유지의 추적과 이를 통한 공격 근원지의 발견, 역추적을 위한 공격근원지의 취약성 탐지와 이를 기본으로 하는 에이전트의 잠입, 에이전트의 자율적 수행과 에이전트들 사이의 협력을 위한 통신의 기능으로 대표될 수 있다.



[그림 1] 능동적 해킹 대응 역추적 에이전트 시스템 설계도

1) 초기 침입 발견

수행 서버 시스템은 독립적으로 자신의 시스템으로의 침입을 감시하기 위하여 두 개의 센서들을 가지고 있는 IDS를 가진다. 하나의 센서는 감사 데이터(audit data)들을 모니터 하는 기능을 가지며 나머지 하나는 네트워크 패킷을 모니터 하는 기능을 가진다. 정상 상태의 서브 시스템에서는 IDS에 의해서 시스템 로그 및 패킷을 모니터 한다. 예를 들어 IDS에 의하여 서브 시스템 상에서의 루트 권한의 획득을 위한 시도 또는 시스템 파일의 변경 등과 같은 의심스런 데이터를 발견하였을 경우 즉시 수행 서버로 통지함과 동시에 수행 서버는 침입이 발견된 서브 시스템의 작업에이전트를 활성화시킴으로써 침입자에 대한 정보들을 수집할 수 있다. 따라서 각각의 작업에이전트에 의해 보내진 정보를 통해 실시간 역추적이 가능할 수 있다 [그림 2].

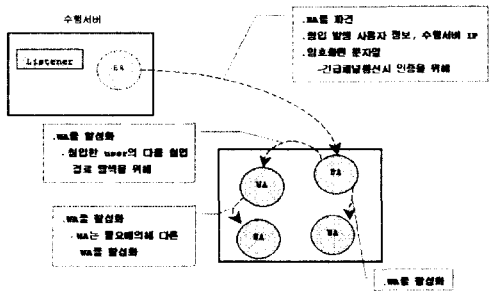


[그림 2]서브 시스템의 침입자 발견에 대한 초기 대응

2) 역추적 에이전트의 파견

서브 시스템으로부터 침입 여부의 판별을 위하여 수행 서버 시스템은 센서들에 의하여 전송된 데이터에 의해 기지 에이전트를 이전 경유지로 이동시킨다. 역추적 에이전트는 이동 에이전트(mobile agent)로써 그 크기가 경량화 되어있으며 자신의 누적 이동 경로를 포함하고

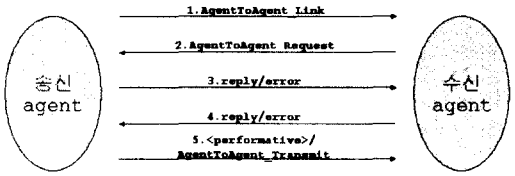
있는 에이전트이다. 이동한 역추적 에이전트는 즉시 작업 에이전트를 활성화한다. 작업 에이전트는 역추적을 위한 이전 경유지 또는 공격의 근원지에 관한 정보를 수집하여 기지 에이전트에게 전송함과 동시에 에이전트 고유의 지식을 기반으로 하여 수집된 데이터를 수행 서버로 전송한다. 이렇게 작업 에이전트에 의해 수집된 정보를 통해 기지 에이전트는 다음 경유지를 결정하게 되고 결정된 경유지로 이동하게 된다. 이후 이러한 절차를 반복 수행함으로써 기지 에이전트는 연속적으로 공격 근원지까지 이동하여 간다 [그림 3].



[그림 3] 에이전트가 활성화된 역추적 시스템

3) 에이전트 및 메시지 보호

에이전트기반 시스템을 구현하는데 있어서의 문제점은 에이전트의 안전한 이동 및 통신이다. 본 연구에서는 에이전트의 이동 및 보호를 에이전트와 에이전트, 에이전트와 수행 서버, 긴급통신의 세 가지 형태로 구분하였다. 에이전트의 통신은 기본적으로 KQML로 설계를 하였기 때문에, KQML상에서의 보안 매커니즘을 설계하였다. KQML 프로토콜은 자체적인 보안 메커니즘의 결여 문제로 인하여, 통신상에 전달되는 메시지의 보안 및 보호의 취약성뿐만 아니라 에이전트 상호간의 인증 취약성을 드러낸다. 이러한 문제점을 해결하기 위해서, 본 시스템에서는 에이전트간의 상호 인증을 위해 기존의 KQML 프로토콜에 새로운 퍼포머티브와 매개 변수를 추가함으로써 메시지 보호 및 에이전트 상호간의 인증을 할 수 있는 구조로 설계하였다. 예를 들면 가장 빈번하게 이루어지는 에이전트간의 메시지 교환 시에 상호인증을 위해 다음과 같은 통신 프로토콜을 이용해 에이전트간의 인증 메커니즘이 수행된다 [그림 4].



[그림 4] 에이전트 인증 메커니즘

5. 결론

본 논문에서는 역추적을 통해서 해킹에 능동적으로 대처할 수 있는 시스템을 멀티 에이전트의 개념을 도입하여 설계하였다. 본 시스템의 기본 설계는 역추적 과정의 가상 시나리오를 바탕으로 하여 상위 레벨에서 이루어졌으며 하부에서 필요로 하는 핵심 요소 기술은 해결된 것으로 가정하였다.

현재 계속 진행되고 있는 연구는 에이전트의 보호를 위한 상위 레벨에서의 전략 및 에이전트간의 안전한 통신을 위한 프로토콜의 정의인데, 상위 레벨에서의 에이전트 보호 전략은 자율 에이전트의 특징을 이용해 에이전트 스스로 판단할 수 있도록 지식의 표현, 전달, 공유, 인퍼런스 등에 관해서 연구하고 있으며 안전한 통신을 위해서는 KQML의 performative의 확장을 고려하고 있다.

참고문헌

[1] M. Genesereth, R. Fikes, "Knowledge interchange format version 3.0 reference manual", Technical Report Logic-92-1, Computer Science Department, Stanford University, 1992.

[2] T. Finin, R. Fritzson., "KQML as an agent communication language." Proc. of CIKM '94, pp 126-130, 1994.

[3] S. Bird, "Toward a taxonomy of multiagent systems", Int. J. of Man-Machine Studies, Vol. 39, pp 689-704, 1993.

[4] P. Cohen, A. Cheyer, A. Wang, S.Baeg, "An open agent architecture", Working Notes of AAAI Spring Symposium on Software Agents, pp 1-8, 1994

[5] M. Asaka, S. Okazawa, A. Taguchi, S. Goto, "A Method of Tracing Intruders by Use of Mobile Agents", INET '99, June 1999.

[6] J. Sundar Balasubramaniyan, J. Omar Garcia-Fermandez, D. Isacoff, E. Spafford, and D. Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents", Tecnical Report 98-05, COAST Laboratory, Purdue University, West Lafayette, In 47907-1398, May 1998.

[7] Guy G. Helmer, Johnny S. K. Wong, Vasant Honavour, and Les Miller, "Intelligent Agents for Intrusion Detection", In Proceeding, IEEE Information Technology Conference, pp 121-124, Syracuse, NY, USA, September 1998.

[8] Guy G. Helmer, Johnny S. K. Wong, Vasant Honavour, and Les Miller, "Lightweight Agents For Intusion Detection", Submitted to Journal of Systems and Software, 2000.

[9] C. Thirunavukkarasu, T. Finin, J. Mayfield, "Secret Agents - A Security Architecture for the KQML Agent Communication Language", Proc. of CIKM '95 Intelligent Information Agents Workshop, 1995.