이동 에이전트를 사용한 보안 취약점 진단 및 모니터링 시스템의 설계

김영균° 오길호
금오공과대학교 컴퓨터공학부
(ygkim, gilho)@cespc1.kumoh.ac.kr

Design of a Security-Vulnerability Diagnosing and Monitoring System using Mobile Agents

Young-Gyun Kim° Gil-Ho Oh
School of Computer Engineering, Kumoh National University of Technology

요 약

네트워크 기술의 보편화로 인하여 분산 네트워크 환경에서의 호스트들은 보안 사고의 위험에 항상 노출 되어 있다. 기존의 보안 기술들은 관리자가 보안을 필요로 하는 호스트에 대해 보안 취약점을 찾아서 이에 대해 조치를 취하는 것이 일반적인 방법이다. 이러한 방법들의 문제점은 새로운 보안 사고 유형에 대해 실시간으로 대처할 수 없을 뿐만 아니라, 관리자의 능력 범위 밖에 있는 호스트들은 항상 무방비 상태로 놓여 있는 문제점들이 있다. 본 논문에서는 이동 에이전트 시스템을 사용하여 각 호스트에 특정 보안 유형에 대해 진단 기능을 갖는 이동 에이전트를 파견하고 보안 취약점을 검사한 후 이를 관리자에게 보고 하는 자동화된 보안 취약점의 진단 및 모니터링 시스템에 대해 연구하였다.

1. 서론

최근 인터넷 등의 네트워크 기술의 보편화로 인하여 네트워크 상의 호스트들을 항상 보안 사고의 위험에 놓여 있다. 기존의 보안 기술들과 방법들은 네트워크 관리자 또는 시스템의 관리자가 관리하는 호스트들에 대해 보안 취약점을 찾아서 이에 대해 조치를 취하는 방법이다.

이러한 방법들의 문제점은 새로운 보안 사고에 대해 실시간으로 대처할 수 없을 뿐만 아니라, 관리자의 부주의로 인한 보안 취약점들에 대해서는 점검과 대책이 어려운 문제점이 있다. 또한 지역 네트워크 내에 많은 호스트들이 연결되어 있는 경우, 모든 보안상의 취약점을 관리자가 찾아서 보완한다는 것은 어려운 실정이다. 따라서, 자동화된 보안 취약점의 모니터링 시스템이 필요로 한다.

본 논문에서는 이동 에이전트(Mobile agents)를 이용하여 네트워크 상의 각 호스트의 보안 취약점을 점검하는 자동화된 보안 모니터링 시스템을 제안 한다.

이 시스템은 보안 취약점의 진단 기능을 갖는 이동 에이전트가 네트워크 상의 각 호스트를 방문하여 방문한 호스트의 보안 취약점을 진단하고 이를 호스트의 사용자 및 관리자에게 알려 주는 방법으로서 보안상의 취약점들에 대해 점검이 용이하고 즉각적인 대책을 수립할 수 있게 한다.

관리하는 호스트가 많은 경우, 또는 관리자와 보안 관리자가 겸임하여 있는 경우의 관리자의 부주의로 인한 보안상의 취약점을 찾기 어려운 점을 본 논문에서 제안한 방법에 의하여 쉽게 해결할 수 있다. 또한 새로운 보안 사고 유형에 대해 실시간으로 대책을 수립할 수 있는 장점이 있다.

2. 관련 연구

최근 들어 전자상거래, 인트라넷, 클라이언트/서버 등의 개방된 인터넷 환경으로 인하여 해킹 등의 시스템의 불법적인 사용으로 인한 피해 사례가 증가하고 있다. 보안에 관한 시스템의 취약점을 보완할 수 있도록 웹 기반의 온라인 취약점 진단에 대하여 연구되었다[1]. 또한 한국 정보 보호 센터에서도 K-COPS라는 보안 점검 서비스를 제공 한다[2]. 해킹 피해 시스템을 자동으로 분석해 주는 AIAA(Autonomous Intrusion Analysis Agent)와 자동 역공격 기술과 에이전트 기술을 이용하여 실시간으로 침입자의 경로를 역추적 하는 시스템에 대한 연구가 진행되었다[3].

그러나,이 연구도 에이전트 기술을 적용하고 있으나 이동 에이전트를 이용한 시스템이 아니기 때문에 새로운 해킹 및 보안 취약점에 대해서는 실시간 대응이 어려운 문제점이 있다.

최근에 발생하는 해킹 사고의 대부분이 스캐닝 도구를 사용하여 공격하고자 하는 시스템의 취약점 정보를 수집한 다음 이를 바탕으로 시스템에 대한 공격을 시도하고 있다. 시

스템의 취약점을 조사하여 분석하는 도구로서 여러 스캐닝 도구들이 배포되었고, 특히 SAINT나 SATAN 등의 도구의 경우에는 웹 기반 취약점 탐지 도구로서 훨씬 쉽게 분석할 수 있지만, 오래되어 효과가 없는 취약점을 점검하기 때문에 최근의 취약점 진단에는 부족한 점이 있다[1]. 시스템의 취약점 분석과 역공격 기법에 관한 연구 외에도 피해를 입은 후에 시스템의 자료 손실에 대한 효과적인 피해 복구를 위한 백업 메커니즘에 대한 연구도 이루어졌다[4].

이동 에이전트(Mobile Agent)는 네트워크상의 호스트를 자율적으로 이동하면서 특정한 작업을 수행하는 프로세스(Process) 이다[6]. 기존의 이동 에이전트를 사용한 보안에 관한 연구는 주로 이동 에이전트와 이동 에이전트 시스템의 신뢰성 있는 인증 또는 이동 에이전트간에 상호 인증 구조[5]에 대해 연구되었다. 본 연구는 이동 에이전트 기반의 다중 에이전트(Multi-agent)를 사용 함으로서 다중 지점(Multi-Host)에서의 보안 취약점에 대해 동시에 실시간으로 분석 및 모니터링이 가능한 특징을 갖는다. 연구에 사용된 이동 에이전트 시스템은 네트워크 상의 이질적인 호스트간에 이동성과 이동한 시스템에서 작업을 수행할 수 있는 자율성과 다중 에이전트 기능을 제공하는 IBM의 Aglet 시스템을 사용하였다. IBM의 Aglet은 Java기반의 이동 에이전트 시스템으로서 이질적인 환경에서 수행이 가능하다[6].

3. 이동 에이전트 기반의 보안 취약점 진단 및 모니터링 시스템(DiaMonds)

시스템은 보안 서버인 DiaMonds(Diagnosing & Monitoring Distributed Security-vulnerability), 보안 진단 기능을 갖는 이동 에이전트인 COPS, 보안 진단 결과에 따라서 패치(Patch) 코드를 자동으로 설치 해주는 PIA(Patch Install Agents)로서 구성이 되고 그림 1의 구조를 갖는다.

제안한 DiaMonds 시스템의 구성은 그림2와 같이 DiaMonds 서버와 진단 및 모니터링 대상인 호스트로 구성이 되고, 서버와 호스트 사이를 보안 진단 및 모니터링 에이전트인 COPS와 패치 자동 설치 이동 에이전트 PIA가 이동하면서 작업을 수행 한다. 관리 대상이 되는 각 Host들은 JVM(Java Virtual Machine)과 이동 에이전트 시스템을 수행하고 있다고 가정한다.

DiaMonds 서버는 절차1과 같은 순서로 수행 한다. 중앙에 있는 보안 서버인 DiaMonds Server는 보안 정보 데이터베이스로부터 보안 유형에 대한 정보를 참조하여 관리자가 설정한 보안 정책에 따라서 보안 진단 기능을 갖는 이동 에이전트인 COPS를 각각의 호스트에게 파견하여 호스트상의 보안 취약점을 파악한다.

COPS 이동 에이전트는 특정 보안 취약점에 대해 진단할 수 있는 기능을 갖고 있다. 파견된 COPS 이동 에이전트는 관리 대상이 되는 네트워크상의 호스트를 차례로 방문하면서 보안 취약점을 진단하고 파악된 보안상의 취약점을 Server에게 전송한다. 파견된 이동 에이전트는 보안 취약점을 특정 호스트에 대해 파악하고 DiaMonds Server에게 전송한 후 현재 호스트에 방문 시간과 점검일지 기록을 남긴 후 네트워크 상의 다른 호스트에 대해 보안 취약점 진단을 수행 하기 위해 다른 호스트로 이동 한다. 이동한 후 동일한 작업을 반복 수행 한다.

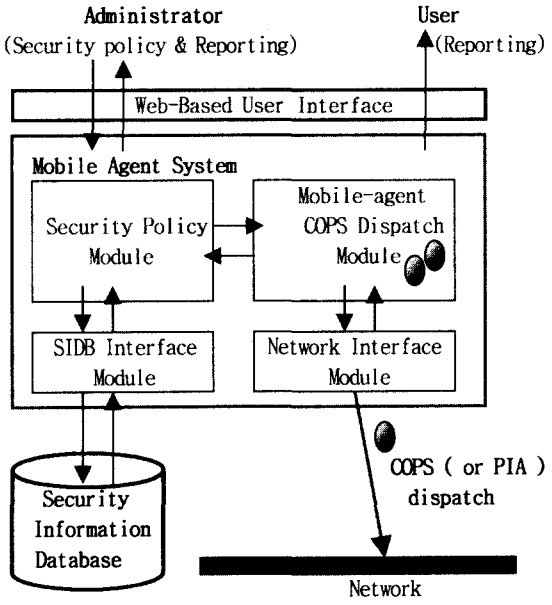

그림 1. 이동 에이전트 기반의 보안 진단 및 모니터링 시스템 DiaMonds

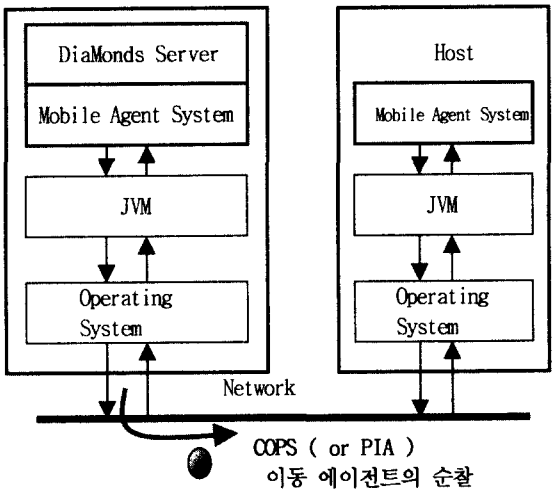

그림 2. DiaMonds 시스템의 구성

DiaMonds서버는 COPS 이동 에이전트의 보안 문제점에 대한 진단 결과를 토대로 보안 정보 데이터베이스(Security Information Database)를 참조하여 호스트의 관리자 및 사용자에게 취약점과 그에 대한 조치 방법을 제안 한다.

DiaMonds 서버는 COPS 에이전트의 진단 결과에 따라서 진단 결과에 대한 모니터링만 할 것인지 아니면 패치 코드를 자동으로 설치하기 위해 PIA 이동 에이전트를 파견할 것인지를 DiaMonds서버의 관리자가 설정한 보안 정책에 따라서 결정한다. 보안 정책 모듈(Security Policy Module)은 관리자가 설정한 보안 정책에 따라서 보안 진단 이동 에이전트를 파견할 호스트를 결정하고, 이동 에이전트 파견 모듈

(Mobile-agent COPS Dispatch Module)에게 파견을 지시하게 한다. 보안상의 취약점을 갖는 호스트에게는 보안 정책 모듈이 패치 코드를 설치하기 위해 PIA를 파견하게 된다.

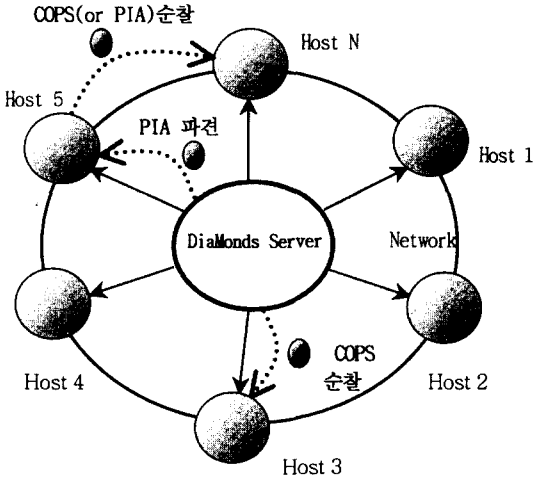

그림 3. DiaMonds 시스템의 보안 진단 이동 에이전트 COPS의 순찰

보안정보 데이터베이스는 보안 취약점의 각 유형별로 특징과 조치 방법에 대한 정보를 담고 있다. 예를 들어,OS종류에 따른 취약한 네트워크 포트, 버퍼 오버 플로우, RPC 취약점 점검, BIND, Sadmin 취약점 점검 등에 관한 특징과 패치 코드 등의 정보를 담고 있다.

절차 1. DiaMonds 보안 진단 및 모니터링 시스템의 수행

Step 1. 설정된 감시할 호스트에게 설정된 보안 정책에 따라서 COPS 보안 진단 이동 에이전트를 파견 한다.
Step 2. COPS 에이전트의 진단 결과에 따라서 PIA 에이전트의 파견 유무를 결정 한다.
Step 3. 파견된 PIA 에이전트는 해당 호스트에 패치 코드를 자동으로 설치 한다.
Step 4. DiaMonds 서버는 진단 결과와 조치 결과를 관리자에게 모니터링 한다.
Step 5. DiaMonds 서버는 계속해서 Step 1부터 반복 수행 한다.

DiaMonds 시스템은 그림 3과 같이 다중의 COPS 또는 PIA 이동 에이전트를 감시 대상 호스트에게 동시에 파견 할 수 있고, 파견된 이동 에이전트로부터 실시간으로 수집된 정보를 기반으로 모니터링을 수행 한다.

새로운 보안 취약점에 대해서 진단 기능을 갖는 COPS 이동 에이전트를 각 호스트에 파견 함으로서 신속한 취약점 분석이 가능하고, PIA 이동 에이전트를 사용 함으로서 실시간으로 다중 호스트에 패치 코드를 자동으로 설치 할 수 있다. 관리자 및 사용자는 웹 기반의 사용자 인터페이스를 통해서 COPS 이동 에이전트의 호스트별 점검 주기 및 보안 정책과 보안 수준, 진단할 호스트의 유형 등에 대한 관련 정보들을 설정할 수 있다.

표1. DiaMonds 시스템의 보안정보 데이터베이스의 구조

No.	필 드 명	설 명
1	Security_Kind	보안 취약점 유형
2	COPS_Type	등록된 보안 진단 이동 에이전트
3	PIA_Type	등록된 패치 설치 이동 에이전트
4	Visit_Period	보안 취약점 진단 주기
5	OS_Version	진단할 OS 버전
6	Host_Type	진단할 Host 유형
7	Security_Char	보안 취약점의 특징
8	Register_Date	보안 유형 등록일자

새로운 보안 취약점이 발견되거나, 네트워크상에 새로운 호스트가 추가된 경우 DiaMonds Server에만 COPS에이전트와 PIA에이전트를 구성해 두면 네트워크상에 있는 모든 감시 대상 호스트에 대해 실시간으로 패치 코드를 자동 설치 한다. 따라서, 각 호스트의 사용자는 DiaMonds 서버에 등록만 함으로서 알려진 보안 취약점 및 새롭게 발견되는 보안 취약점에 대해 호스트마다 사용자의 수작업으로 패치를 설치하거나, 네트워크 상에 있는 호스트의 사용자 부주의로 인한 보안 사고가 다른 호스트의 보안 사고로 전파되는 것을 지속적으로 막을 수 있다. 또한 새로운 호스트가 추가되는 경우와 같이 네트워크의 구성이 변경되어도 자동으로 해당 호스트에 패치가 설치된다는 장점이 있다.

4.결론

본 논문에서 제안한 이동 에이전트 기반의 보안 취약점 진단 및 모니터링 시스템은 인터넷과 네트워크 기술의 보편화 및 고도화가 진행될수록 널리 사용될 수 있을 것이다.
또한, 보안 정보 데이터베이스의 보다 풍부한 사례 구축을 통해서 보다 완벽한 보안 취약점 분석 기술로의 성능 향상을 기대할 수 있으며, 차후, 이동 에이전트에 기반 하여 인터넷 환경에서 보다 자동화되고 지능화된 보안 진단 및 모니터링 시스템에 대해 연구해 보겠다.

참고 문헌

[1] 서현진, 강태호, 이재영, "웹 기반에서 시스템 보안 취약점을 진단하는 시스템", 제27회 한국정보과학회 추계 학술발표 논문집,2000
[2] 한국정보보호진흥원, http://www.kisa.or.kr
[3] 채연주, 서진철, 임채호, 원유헌, "해킹 기법을 응용한 침입자 역추적 시스템", 제27회 한국정보과학회 추계 학술 발표 논문집, 2000
[4] 송병욱, 박보석, 장희진, 김상욱, "전산망 보안관리 통합 시스템에서의 피해 복구를 위한 에이전트 백업 메커니즘", 제27회 춘계 한국정보과학회 학술 논문 발표집, 2000
[5] 백광진, 김태윤, "이동 에이전트를 위한 상호 인증 구조", 한국정보처리학회 추계학술발표논문집 제6권제2호,1999
[6] Danny B. Lange / MITSURU OSHIMA, Programming And Deploying Java Mobile Agents With Aglets, Addison-Wesley, 1998