네트워크 보안관리를 위한 이동에이전트 설계

정현진*, 마복순*, 송성훈**, 임채호***, 원유헌*

*홍익대학교, **혜천대학, ***한국정보보호센터

Design of Mobile Agent for Network Security Administration

Hyunjin Jung*, Bocksoon Ma*, Sunghun Song**, Chaeho Lim***, Yoohun Won*

* Hongik University, ** Hyechon University
*** Korea Information Security Agency

요약

이동에이전트는 인터넷 상거래나 자동검색 등에 응용되는 최근 기술이며 이를 컴퓨터네트워크내 컴퓨터시스템의 보안관리을 위한모델을 제안하고 설계하였다. 이를 위해 최근 발표되고 있는 이동에이전트 기술에 대해 분석하고, 네트워크보안관리 기술을 연구하였으며 IBM이 제안하고 있는 AGLET 환경에 네트워크보안관리 시스템을 탑재한 이동에이전트 응용시스템을 설계하였다.

1. 개요

최근 인터넷을 비롯한 정보통신망에서의 해킹으로 인한 침해사고가 점점 증가하고 있으며[12][17] 이에 따라 인터넷에서의 해킹방지를 위한 각종 대응기술들이 개발되고 있다[13][14][15].

이러한 기술들은 최근 주로 시스템 하나에 설치하여 운영하는 해킹방지를 위한 기술이 아니라 클라이언트/서버 환경에서 동작하는 네트워크보안관리 차원의 기술을 제공하는 방법을 주로 사용하고 있다[13][14].

[표1] 해킹방지기술제품

기술분야	대표 제품/개발자	특 성
보안 취약성 분석	SAFEsuit/ISS, Inc. [12]	-135여개 취약점 검사 -시스템, 방화벽, WWW 서버 점검
전산망 보안관리	OmniGuard/Axent[13] INSA[14]	-클라이언트/서버 환경 -사용자/파일/네트워크 보안정책
전산망 침입탐지	RealSecure[12]	-네트워크 침입탐지 -공격 패턴 트래픽분석 -실시간 공격인지대응

최근 웹기반의 검색대행시스템이나 전자상거래 등에서 활용되기 시작하고 있는 이동에이전트기술은 네트워크 보안관리 등에 활용할 수 있는데, 이러한 방안을 응용하여 보안관리기술에 적용할 수 dT을 것으로 분석하였다.

본 연구에서는 이동에이전트 기술을 전산망기반의 보안관리기술에 적용하기 위한 기본 모델을 연구하였다. 이는 기존의 고정적인 C/S 개념의 보안관리 기술을 이동에이전트에 적용한 모델을 제시하여 이동에이전트 응용의 한 분야를 제시하는 것으로 본 연구의 기본 목표로 삼았다.

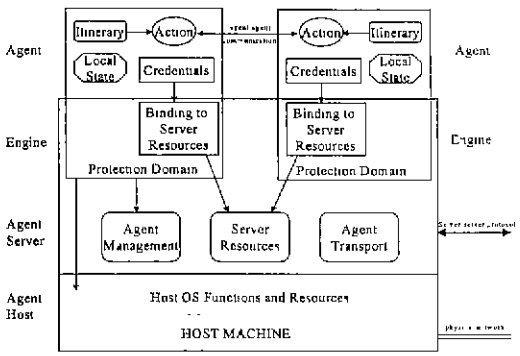
본 연구를 위한 이동에이전트 및 전산망보안관리 기술 등 기본연구사항, 모델링 및 설계 등을 설명한다.

2. 관련연구

2.1 이동에이전트 기술 분석[1][2][3][4]

이동에이전트(Mobile Agent)는 독립적이고 자의적으로 이벤트가 발생했는지의 여부를 볼 수 있고, 인터넷 상에서 사용자가 원하는 정보가 어디에 있는지 돌아다니며 탐색할 수 있고, 여러 가지 서비스를 종합적으로 처리할 수 있다. 이러한 응용으로는 전자상거래, 그룹작업, 이벤트모니터링, 정보검색, 흐름자동화, 망관리, 이동컴퓨팅[8] 등에 활용될 수 있다.

다음 <그림1>은 이동에이전트의 기본 개념을 설명하고 있으며, [표2]는 최근 관련 기술개발 현황을 보여주고 있다.



<그림 1> 이동 에이전트 구조

이동 에이전트 기술은 세가지 주요한 요소를 가진다. 첫 번째 요소는 에이전트 프로그래밍 언어이다. 에이전트 프로그래밍 언어는 개발자가 에이전트와 에이전트가 방문할 플레이스를 프로그램 하

게 해준다. 두번째 요소는 에이전트 시스템으로 에이전트 언어를 위한 가상기계를 제공하며 에이전트와 플레이스의 동작을 관리한다. 그리고, 마지막 요소는 에이전트 프로토콜로서 에이전트끼리 서로 다른 컴퓨터 시스템사이에서 통신을 가능하게 해주는 것이다.

[표 2] 최근 에이젼트 시스템 개발현황

이동 에이전트 기술명	개 발 자
Aglets Workbench	IBM
Agentware Suite,	Autonomy
Agents for Remote Action	University of Kaiserslautern
Caltech Infospheres Infra..	Infospheres Groups
Cobalt	Dominiq Benech
Concordia	Mitsubish Electric Information Tech Center America
FTP Software Agent	FTP
Guideware SDK	Guideware
Java Agent Template	H. Robert Frost
JATLite	Stanford University
MESSENGERS	University of California
MOA	OpenGroup
Mobile Service Agent	ECRC
Mole	Mole Team
Odyssey	General Magic
Voyager	ObjectSpace

이동에이전트를 구현할 수 있는 언어들로는 Java, Telescript, Obliq, Safe-Tcl, Agent-Tcl, TACOMA등이 있으며 이들의 특징을 다음 [표 3]에서 설명하고 있다[9].

[표 3] 이동에이젼트언어 종류

언어명	특 징
Java	이식성과 안전성, 정보보호 기능이 뛰어남 포인터, 다중상속 개념을 삭제하여 간략화
Telescript	순수 객체 중심언어로 전자상거래 분야를 목표로 정보보호와 에이전트기능 중심
Obliq	분산 객체 중심 컴퓨팅을 지원하기 위해 DEC사에서 개발된 순수 인터프리터 언어
Safe-Tcl	Tcl을 확장한 언어
Agent-Tcl	Tcl 인터프리터를 확장하여 명령어 하나만으로 코드 이동을 지원하는 언어

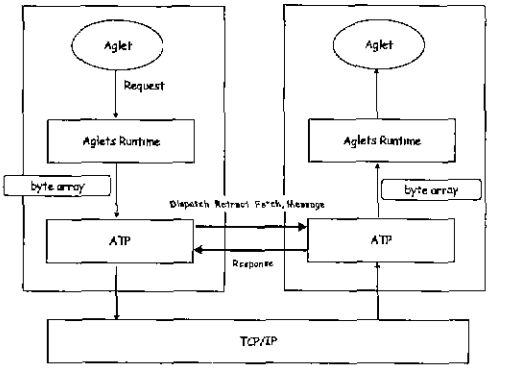
2.2 IBM Aglets 분석[5][6][7]

Aglets은 지역데이터와 다른 정보들을 찾고, 제어하고, 관리하기 위해 이동 에이전트를 사용하는 네트웍 기반의 어플리케이션을 작성하기 위한 시각적인 환경을 제공하는 도구이다. Aglets 은 자바 프로그래밍 언어를 기반으로 한 플랫폼에서 독립적인 이동에이전트 작성을 기존의 방법보다 훨씬 더 쉽게 해준다. Aglet의 Visual Builder는 Internet을 돌아다닐수 있는 개인화된 에이전트를 빠르게 구성하도록 해준다. 또한 Aglet의 풍부한 소프트웨어 요소들의 집합들이 에이전트가 데이타베이스의 제어나 탐색, 여행, 표준화된 통신을 가능케한다

Aglets의 핵심은 Aglet 프레임워크로서 자바 프로그래밍언어 시스템을 기반으로 하고 있으며 이동에이전트에 필요한 고유한 요소들을 제공한다. Aglet 클래스(class)를 사용하는 것은 사용자 정의 에이전트가 이동 에이전트 구현을 위해 부족한 속성과 기능을 상속받기 위한 평범한 방법이다.

2.3 네트워크 보안관리 분석

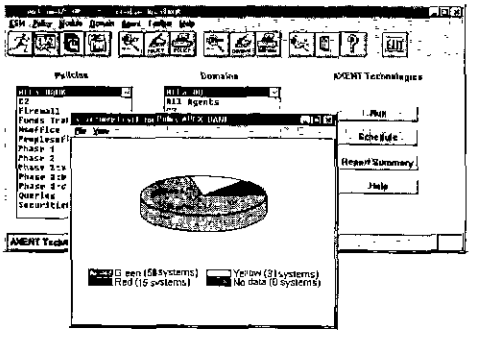
네트워크에서의 보안관리는 주로 네트워크에 접속



<그림 2> Aglet 구조

된 정보시스템이 보안상태를 관리하는 것으로 보고 있으며 설정한 보안정책에 따라 시스템이 잘 구현관리되고 있는지, 긴급사안은 없는지 관리하는 것이 대표적인 방법이다.

<그림3>은 네트워크 보안관리시스템의 대표적인 제품인 Axent사의 옴니가드(OmniGuard)의 실행화면 예제를 보여주고 있는데 시스템의 보안속성 상태를 주기적으로 점검하여 관리자에게 GUI 기반으로 디스플레이하여 주는 것이다.



<그림3> OmniGuard 실행화면

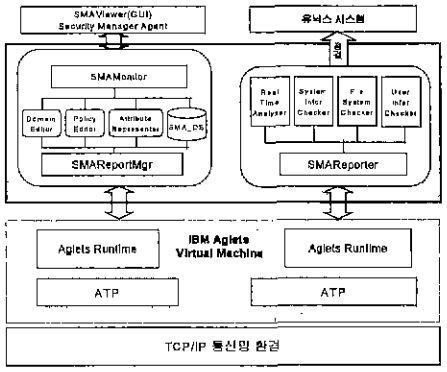
한국정보보호센터에서는 해킹방지 관련 국내기술개발을 위해 클라이언트/서버 환경에서의 정보시스템 보안관리 기술개발을 일부 수행한 바 있다[10]. 이 기술은 시스템의 보안정책 위반을 모니터하는 에이젼트SW가 클라이언트시스템에 고정적으로 설치되어 주기적으로 서버에 보고하여야 한다.

모니터링하는 보안속성은 유닉스 에이젼트의 계정무결성, 백업무결성, 파일접근제어, 파일속성, 파일찾기, 로그인 파라메타, 객체무결성, 패스워드 안전성, 시작파일, 전자우편, 시스템감사기록, 시스템큐, 사용자파일 등의 보안대상 자원이다.

3. 구현 시스템 모델 및 설계

3.1 목표시스템 모델

다음 <그림4>는 전산망보안관리를 위한 이동에이전트 설계를 위한 모델을 보여주고 있다. 기본적으로 TCP/IP 인터넷 환경을 이용하는 IBM Aglet 가상기계 환경을 이용하여 동작하는 이동에이전트 응용시스템을 구현한다. SMA는 Security Management Agent 의 약자이다.



<그림 4> 보안관리이동에이전트 설계 모델

3.2 보안관리에이전트(SMA) 동작 개념

시스템은 IBM Aglets 가상기계상에서 동작되며, SMAViewer를 통하여 SMA의 보안정책들을 설정하며, SMAMonitor의 모니터링 표현방식(텍스트, 테이블, 챠트)을 결정할 수 있다. 설정된 내용은 SMAReportMgr가 Aglets 가상머신에게 에이전트의 생성을 의뢰하여 가상머신이 SMA를 생성하고 대상호스트로 파견한다. 파견된 에이전트는 호스트에 도착하여 실시간점검, 시스템 정보 점검, 계정점검, 파일시스템 점검 등의 기능을 수행하여 SMAReportMgr로 보고하게 되고 Sec_DB에 결과가 저장된다. 파견된 SMA는 대상호스트가 끝날 때 까지 연속이동한다.

또한 SMAMonitor 는 사용자가 설정한 표현방법에 따라 Sec_DB에 저장된 각 호스트의 보안상태 정보를 가공하여 관리자에게 디스플레이 하게 된다.

SMAViewer는 관리자가 SMA를 제어하고 결과를 보고 받을 수 있는 사용자 인터페이스 기능만 제공하며 파견하고자 하는 에이전트의 영역설정, 보안 정책, 보안속성값들의 표현에 대한 설정은 실제로 SMAMonitor에서 수행된다.

SMAMonitor에서 설정한 사항들을 종합하여 Aglets 가상머신에게 에이전트의 생성을 의뢰하는 것은 SMAReportMgr가 담당한다. Aglet 가상머신은 부탁받은 에이전트를 생성하고 관리하며 파견하는 일을 한다. 에이전트의 생성과 관리는 Aglets Runtime에서, 네트워크 이동시의 프로토콜은 ATP에서 담당한다.

SMA는 한 호스트에서 수행을 마치면 다음 호스트로 이동하고 자신의 스케줄에 따라 이동하며 임무를 끝마친 에이전트는 삭제된다.

4. 결론 및 향후과제

지금까지 이동에이전트를 응용한 전산망보안관리 시스템의 개발을 위한 시스템 모델과 설계를 보았다. 이를 위하여 이동에이전트에 대한 기본연구를 하였고 가장 보편화되고 표준화가 잘 진행되고 있는 IBM Aglet 의 주고와 기능에 대하여 살펴보았다. 그리고 최근 인터넷 보안관리 분야에 가장 각광받고 있는 C/S를 기반으로 하는 OmniGuard 에 대해서도 분석을 하였다.

이러한 분야의 응용과제는 아직 국내외 이동에이전트에서 소개되고 있지 않는 상태이므로 본 연구를 통하여 이동에이전트를 이용한 보안관리를 응용의 하나로서 제시하고자 한 것에 본 연구의 의의가 있다.

추후 이러한 모델을 바탕으로 TCP/IP LAN환경의 유닉스시스템을 대상으로 프로토타입을 구현하여 동작을 검증할 예정이며, 기존의 C/S 타입의 보안관리시스템과 성능을 비교하고자 한다.

또한 이러한 정책기반의 보안관리 뿐 아니라 실시간 침입탐지 등을 적용한 복수개의 이동에이전트를 구현, 해킹 등 침입으로 피해를 입은 시스템의 자동 분석 및 복구 등 응용부분의 기능을 보완 발전하는 것이 하나의 과제라고 본다.

<참고문헌>

[1] Neeran M. Karnik, Anand R. Tripathi, System Support for Mobile Agents
[2] Stan Franklin and Art Graesser, Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agent, Proceeding of the Third International Workshop on Agent Theories, 1996
[3] Steven R.Farley, Mobile Agent System Architecture - A flexible alternative to moving data and code to complete given task, SIGS Publications, 1997,
http://www.sigs.com/publications/docs/java/9705/farley.html
[4] Mobile Agent White Paper, General Magic,
http://www.generalmagic.com/technology/techwhitepaper.html
[5] Bill Venners, Under the Hood: The architecture of aglets, JavaWorld, April 1997,
http://www.javaworld.com/javaworld/jw-04-1997/jw-04-hood.html
[6] Chong Xu, Dongbin Tao, Building Distributed Application with Aglet, http://www.cs.duke.edu/~chong/aglet/
[7] Colin G. Harrison, David M. Chess, Aaron Kershenbaum, Mobile Agenst: Are they a good idea?, IBM Research Report, March 13, 1995
[8] 김평중, 윤석환, "이동 컴퓨팅을 위한 이동 에이전트 시스템", 정보처리 제4권 제5호, 1997. 9
[9] 박지은, 김상욱, "이동 에이전트를 지원하는 프로그래밍 언어", 정보처리 제4권 제5호, 1997 9
[10] 한국정보보호센터, 전산망 종합보안상황 모니터시스템, 1997.12
[11] 한국정보보호센터, 클라이언트/서버에 기초한 보안관리 기본시스템 개발, 1997. 12
[12] 한국정보보호센터, '97 정보시스템 해킹현황 및 대응, 1997. 12
[13] ISS, Inc. 홈페이지, http://www.iss.net
[14] Axent, Inc. 홈페이지, http://www.axent.com
[15] INSA 홈페이지, http://www.tlinet.com
[17] 신 호, 정운종, 임채호, 김종섭, "해킹피해시스템 분석 방법", 1998. 9, WISC'98