이동컴퓨팅 보안기술

홍익대학교 원유헌*

1. 서 론

현재 이동 에이전트를 이용한 전자상거래, 이동 컴퓨팅 및 정보관리, 정보 검색 등의 분야가 활발하게 진행되고 있다. 이러한 이동 에이전트를 이용한 시스템은 사용자의 개입 없이 독립적으로 임무를 수행하여 사용자가 직접적인 운영을 하지 않아도 그 행동을 대신할 수 있는 장점이 있고 정보를 여과하거나 또는 방대한 양의 정보를 체계적으로 수집, 관리할 수 있는 장점을 지니고 있다. 그러나, 새로운 패러다임을 채택하기 위하여 고려해야할 문제로 이동 에이전트의 보안 및 이동 에이전트를 수행하는 호스트의 보안 문제가 제기되고 있다. 이동 에이전트는 네트워크를 통해 원격지의 호스트로 이동하여 부여된 과제를 수행하는데 이때 네트워크 상에서 불법적인 변경이나 공격을 받을 수 있다. 또한 이러한 이동 에이전트가 호스트에 접속하여 악영향을 미칠 가능성을 배제할 수 없다. 특히, 전자상거래와 같은 개인의 신상정보가 요구되는 응용 프로그램에서 사용되는 이동 에이전트는 신분 인증 및 내용상의 유해성 여부를 간과할 수 없다. 따라서 본고에서 이러한 이동 코드의 보안 문제를 해결하기 위한 패러다임을 제안하고 부가적으로 고려해야할 문제들을 설명한다.

2. 이동 에이전트와 보안

2.1 이동 에이전트

이동 에이전트는 이동 분산 환경에서 사용자를 대신하여 주어진 문제의 해결을 위하여 원격지 호스트로 이동하며 어떤 일을 해야하는지를 정해진 규칙에 따라 스스로 결정할 수 있는 자율적인 객체를 의미한다. 이동 에이전트의 특징으로는 다음과 같은 특징이 있다.

- ㅇ자율성(Autonomy) : 자율성은 에이전트와 일반 소프트웨어를 구별해 주는 가장 핵심적인 특징으로 에이전트가 자율성을 가짐으로서 사용자의 지시 없이 스스로 목적을 달성하기 위해서 환경 또는 상태에 의해 독립적으로 자신의 행동을 결정한다. 즉 사용자의 요구에 따라 그것을 달성할 책임이 있고 스스로 활동하는 능력이 포함되어 있다.
- ㅇ지능성(Intelligence) : 에이전트의 지능성은 자율성의 바탕이 되는 특성으로, 이를 위해 에이전트는 지식 베이스를 채택하고 있으며 추론 및 계획 능력을 가지고 있다
- ㅇ반응성(Reactivity) : 어떠한 환경에 위치하여 환경을 지각하고 변화하는 환경에 반응할 수 있다.
- ㅇ이동성(Mobility) : 사용자가 요구한 작업을 현재의 플랫폼에서 수행하지 않고 그 작업을 수행할 수 있는 다른 호스트로 이동하여 작업을 수행한다
- ㅇ사회성(Socialability) : 에이전트는 자신의 목표를 이루기 위해 다른 에이전트와도 상호작용을 통해 정보를 교환한다.

2.2 이동 에이전트 시스템

대부분의 통신 환경이 되고 있는 클라이언트/

* 종신회원

서버 환경에서는 통신 소프트웨어 모듈간의 분산 처리가 RPC(Remote Procedure Call)에 의해 이루어지는 반면에 이동 에이전트 환경에서는 실행 프로그램이 실제로 데이터가 존재하고 있는 장소로 이동하여 수행하는 방식, 즉 데이터를 이동시키지 않고 에이전트 자신의 프로그램 코드가 이동하는 방식을 이용한다.

이동 에이전트 기술에서는 네트워크를 에이전트 서버로 동작하는 플레이스(place)들의 집합으로 보며, 이들 장소들은 자신에게 들어오는 이동 에이전트들에게 서비스를 제공하게 된다. 이동 에이전트를 구성하는 기반 기술은 다음과 같다.

- 플레이스(Place) : 에이전트를 실행시킬 수 있는 에이전트 시스템의 실행 환경을 제공하며, 이동 에이전트의 출발점과 도착점 기능을 제공한다. 이동 에이전트를 받아들여 수행환경을 제공하며, 호스트의 자원을 활용하도록 해주거나 사용자 인터페이스를 제공한다.
- 이동에이전트(Mobile Agent) : 에이전트의 활동이 시작된 플랫폼에 고정되지 않고, 자율적으로 한 장소에서 다른 장소로 이동하며, 서로 다른 시간에 서로 다른 장소를 점유한다.
- 통신기반(Communication Infrastructure) : 이동 에이전트의 통신을 담당하는 하부 기반 구조로서 RPC, RMI(Remote Method Invocation) 등이 있다.
- 플랫폼(Platform) : 에이전트 시스템이라고도 하며, 이동 에이전트를 생성, 이동, 수행, 전송, 해석 및 폐기 등 에이전트를 관리 할 수 있는 시스템이다.
- 전송(Transfer) : 이동 에이전트가 하나의 에이전트 플랫폼에서 다른 에이전트 플랫폼으로 이동하는 기능이다. 이동은 에이전트가 다른 에이전트 플랫폼에서 제공된 서비스를 제공받기 위하여 필요한 때 이루어진다. 이를 위하여 에이전트의 상태가 이식되어 처리가 가능해야 한다.

2.3 공개키 기반 디지털 다중 서명에 의한 에이전트 인증

종래의 비밀키(혹은 대칭키)암호 방식은 두 통신 당사자가 같은 비밀키를 공유해야만 비밀보장이나 인증 등과 같은 보안 서비스를 이용할 수 있다. 따라서 비밀키 암호 방식은 키 분배 문제로 인해 인터넷과 같은 공개 통신망에서 사용하기에는 신뢰관계의 구축이나 확장성 등이 어렵다는 문제점이 있다. 이러한 키 분배 문제를 해결해 줄 수 있을 뿐만 아니라 통신망상의 거래에서 가장 중요한 기능인 디지털서명을 제공해 줄 수 있는 암호 기법이 공개키(혹은 비 대칭키) 암호 방식이다. 공개키 암호에서는 공개키를 모든 사용자들이 알 수 있게 공개하고 비밀키는 그 자신만이 간직하게 된다 따라서 공개키 암호 방식에서는 통신 당사자의 공개키만 알면 모든 보안 서비스를 제공받을 수 있다. 그러나, 공개키 암호를 이용하기 위해서 가장 중요한 것이 상대방의 정확한 공개키를 얻는 것이다.

공개키 기반구조(Public Key Infrastructure : PKI)란 이와 같이 공개키 암호 방식을 사용하는데 필요한 기본적인 서비스를 제공하기 위해 구축되는 기반구조를 의미한다. 가장 기본적인 것이 임의의 원하는 상대방의 정확한 공개키를 얻을 수 있는 메커니즘이며, 부가정보로는 디지털 문서에 대한 공증이나 디지털 등기 메일 등 다른 다양한 서비스를 제공할 수도 있다. 정확한 공개키의 분배를 위해 가장 널리 사용되는 것이 신뢰할 수 있는 공개키 인증 기관(Certification Authority:CA)에서 각 사용자의 개인정보와 그의 공개키 등을 결합하여, 디지털 서명한 공개키 확인서(Public Key Certificate, 혹은 간단히 Certificate)를 발행하여 이를 모든 다른 사용자들이 이용할 수 있도록 공개키 디렉토리 등의 형태로 운영하는 것이다. 그러면 사용자들은 상대방의 공개키 인증서를 입수하여 CA의 서명을 검증함으로써 그 공개키가 원하는 상대방의 공개키인지를 확인할 수 있다. 따라서 공개키 기반구조에서 가장 중요한 것이 공개키 확인서의 발행이나 취소 및 분배 등과 관련된 확인서 기능과 다수의 CA들간에 신뢰관계를 구축하는 일이라 할 수 있다. 공개키 확인서는 X.509에서 표준화된 형식이 가장 널리 사용된다.

2.4 에이전트 연구 동향

2.4.1 FIPA

FIPA(The Foundation for Intelligent Physical Agents)라는 단체는 1996년 9월에 스위스 제네바에서 설립된 비영리단체로서 그 목적은 에이전트를 기반으로 하는 응용 프로그램들의 상호운영을 최대화하기 위한 일반적 에이전트 기술에 대한 사양을 증진하기 위해 설립된 단체이다. FIPA는 이미 1997년에 FIPA97이라는 7가지 사양을 개발하였고 개발작업을 계속 진행 중에 있으며 다음과 같은 전제에서 에이전트의 기술을 평가하고 있다

- ㅇ에이전트는 기술의 완성 시도가 가능한 분야이다.
- ㅇ에이전트 기술을 이용하는 응용 프로그램이 나타나기 시작했다.
- ㅇ여러 경우에 있어서 표준화는 에이전트 기반의 상품이나 서비스 및 응용 프로그램을 폭넓게 발전시키는 요인이 된다.

FIPA에서 제시한 에이전트를 이용한 프레임워크는 다음의 그림 1과 같다.

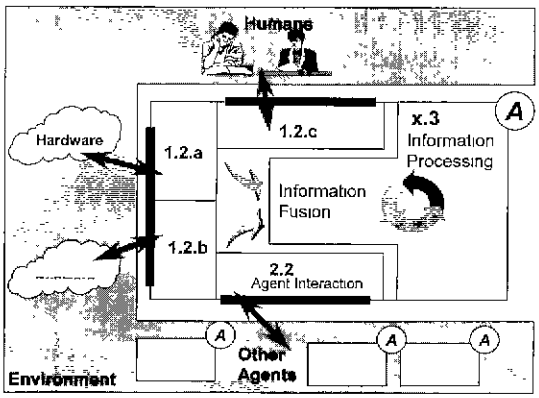


그림 1 FIPA의 Framework

그림 1에서와 같이 에이전트를 이용하여 원격지의 개체와 상호작용을 이루어 낼 수 있고 에이전트를 이용함에 따라 사용자가 직접적으로 대화식으로 처리해야 하는 작업을 수행할 수 있다는 큰 장점을 지니고 있다. 이러한 분야를 다음과 같이 구분하여 살펴볼 수 있다.

- ㅇ사용자 지원 응용(User Assistance Applications)
  - 개인의 전자우편 필터링이나 정렬(Personal Email Filter, Sorter)
  - 개인의 영화나 음악 제공(Personal Movie/Music Recommendation)
  - 개인의 회의 스케줄러(Personal Meeting Scheduler)

- ㅇ정보 검색 응용(Information Retrieval Applications)
  - 디렉토리 서비스(Directory Services)
  - 데이터베이스 질의(Data Base Inquery)
  - 학습 & 적응 시스템(Learning & Adaptive Systems)
  - 정보 중개(Information Brokerage)

- ㅇ서비스 관리 응용(Service Management Applications)
  - 멀티미디어 정보 설비 서비스(Multimedia Information Provision Services)
  - 재정 정보 설비 서비스(Financial Information Provision Services)
  - 매매 정보 서비스(Buing/Selling Information Services)
  - 전자상거래(Electronic Commerce)

에이전트는 나열한 응용 이외에도 수없이 많은 분야에서 이용 가능하다. FIPA의 구체적인 목적은 1)에이전트 관리(Agent Management), 2)에이전트간의 상호작용(Agent/Agent Interaction), 3)에이전트와 소프트웨어의 통합(Agent/Software Integration) 등을 주 골격으로 하여 표준화를 위한 작업을 계속 진행중이다. 이러한 추세는 향후 2-3년 내에 표준화된 명세를 바탕으로 각 응용 프로그램에 이용할 전망이다. 특히, 인터넷 사용자들로 하여금 가장 관심을 갖게 하는 분야는 전자상거래로 많은 인터넷 관련 회사나 단체에서 시도하고 있다.

다음의 그림 2와 그림 3은 에이전트를 이용하지 않았을 경우의 사용자의 정보 습득과정과 에이전트를 이용한 정보 습득 과정을 비교하고 있다. 이전의 사용자는 대화식으로 원하는 정보를 스스로 해결해야만 했으나 이동 에이전트를 이용하였을 경우 사용자가 원하는 자료만을 입력했을 경우 원하는 결과를 에이전트의 습득 데이터를

통해서 얻을 수 있다는 장점을 가지고 있다.

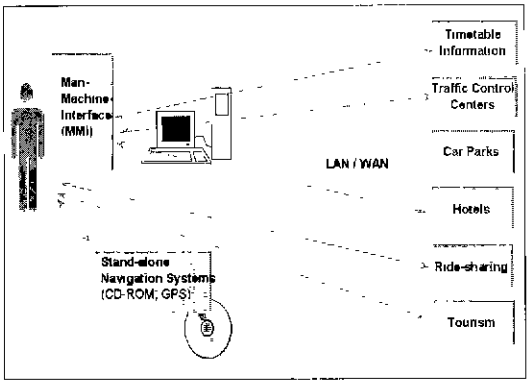


그림 2 에이전트를 이용하지 않았을 경우의 사용자의 정보 습득과정

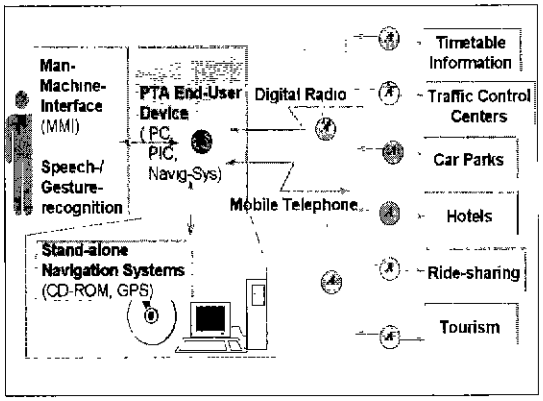


그림 3 에이전트를 이용한 경우의 사용자의 정보 습득과정

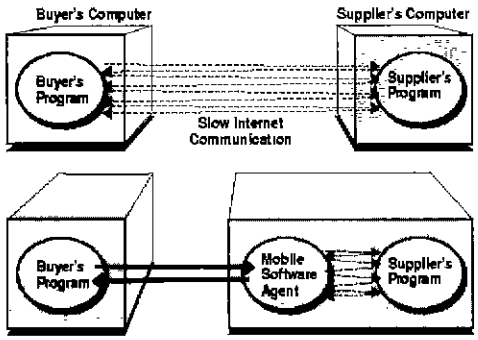


그림 4 인터넷을 통한 상품 거래 방식 비교

2.4.2 전자 상거래 응용

다음 그림 4는 구매자와 판매자가 인터넷을 통해 상품 거래를 할 때 기존의 인터넷을 통한 방식과 에이전트를 사용하였을 때의 방식을 비교하고 있다.

기존의 방식은 구매자와 판매자가 어떤 거래를 위해 지속적인 접근이 필요하지만, 에이전트를 이용한 방식은 구매자가 원하는 상품에 대한 정보 및 가격 등을 에이전트에 포함시켜주면 나머지 거래를 위한 일련의 작업은 에이전트가 수행하게 된다

3. 이동코드보안시스템 설계

3.1 이동 코드 보안 시스템 설계

이동 코드 보안 시스템은 이동코드를 발생하고자 하는 호스트에 전자서명용 인증서를 발급하고 또한 이동 코드가 적용될 서버 시스템에 같은 용도의 전자서명용 인증서를 발급하는 시스템을 말한다. 다음의 그림 5는 전체적인 이동 코드 보안 시스템을 보이고 있다.

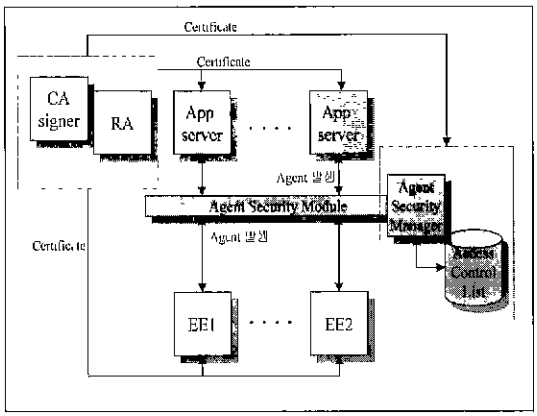


그림 5 이동 코드 보안 시스템

3.1.1 CA 서버

CA 서버는 전자서명용 및 암호용 인증서를 각각의 이동에이전트 관련 호스트에 발급하는 기능을 갖는다. 이러한 인증서는 각 호스트나 서버의 사용자 신분 인증 및 메시지 인증을 위한 수단으로 사용되며 CA의 정책에 따라 등록 및 발

급, 교체 및 폐기를 주기적으로 수행한다.

CA 서버로부터 인증서를 교부 받은 호스트나 서버는 인증하고자 하는 상대 호스트의 인증서를 받아와 인증 및 암/복호화에 이용한다. 본 논문에서는 CA자체에 대한 연구보다는 CA에서 발급하는 인증서의 종류를 분류하여 전자서명 용도를 위한 인증서를 발급만을 취급하도록 한다.

3.1.2 에이전트 보안매니저(Agent Security Manager)

CA Signer에서 발급 받은 인증서를 통해 이동 에이전트는 자신의 신분 인증 및 메시지 인증을 수행한다. 이동 에이전트는 발생 시에 코드 부분과 인증을 위한 서명 부분으로 구성되어 지며 이를 네트워크를 통해 원격지로 전송할 때 코드부분을 원격지의 공개키로 암호화하여 전송한다. 수신된 이동 코드는 우선적으로 상대방의 인증서를 이용하여 신분에 대한 인증을 수행한다. 검증과정에서 문제가 발생하는 경우 즉각 Agent Security Manager로 통보함으로써 에이전트의 실행을 중지할 수 있도록 한다. 이러한 신분 인증을 마친 후 수신한 서버의 비밀키를 이용하여 코드 부분을 복호화하여 이동 에이전트를 실행한다. 이때 이러한 일련의 과정은 Agent Security Manager를 통하여 이루어지는데 이는 이동 코드의 권한제어를 갖추기 위한 방안으로 호스트에서 발생한 이동 코드는 Agent Security Manager에서 1차 인증을 거친 후 해당 서버로 전송된다. 만약 Agent Security Manager가 정상적인 운영을 수행하지 못할 경우 직접 해당 서버로 전송할 수 있는 방안도 함께 고려한다. 이러한 Agent Security Manager를 통한 우회방법은 권한 제어에 대한 방법을 제공하기 위함이고 또한 이러한 방법을 통해 이동 코드의 획일적인 관리를 이끌어낼 수 있다. 또한 Agent Security Manager는 Access Control List를 데이터베이스로 관리하며 각 호스트나 서버에 대한 권한 제어를 처리한다. 권한제어 부분은 이동 코드의 상태필드와 함께 전송되며 권한제어에 따라 서버는 이동 코드를 제어관리 할 수 있는 권한을 얻을 수 있다.

3.1.3 응용서버(Application Server)

에이전트보안매니저(Agent Security Manager)를 통해서나 또는 호스트에서 직접 응용서버로 이동된 에이전트는 인증 과정을 거친 후 Agent 플랫폼에 위치한다. 플랫폼에 위치한 이동 에이전트는 복호화된 코드형태로 호스트에서 수행을 위해 정의된 코드와 에이전트의 상태를 나타내는 상태(State)를 갖는다. 또한 목적지에 대한 정보를 링크드리스트형태로 저장하여 한 서버에서 일을 수행한 후 다음 목적지로의 이동주소를 이 리스트를 통하여 알 수 있다. 그리고 이는 상태변수에 따라 다음의 원격지로 보내어질지 아니면 호스트로 보내어질지를 결정한다. 이를 위하여 Agent Transfer Protocol(ATP)를 사용한다. 이 때 이동 코드를 보내는 응용 서버는 자신의 전자서명을 이동 에이전트에 덧붙임으로써 원격지의 서버로부터 자신에 대한 인증을 추가로 받게 한다. 그림 6은 Application Server의 구성도이다.

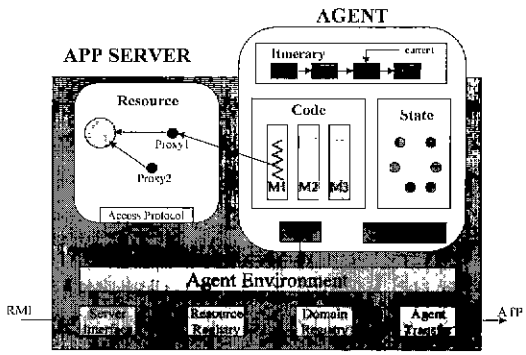


그림 6 Application Server의 구성도

즉, 하나 이상의 원격 서버를 거친 후의 이동 에이전트의 코드는 그림 7과 같다. 우선 실행을 위한 코드와 에이전트를 발생시킨 호스트의 전자서명값을 기본으로 한 후 주어진 일에 따라 데이터가 추가되며 이 때 이 데이터를 생성한 서버나 호스트의 전자서명을 함께 추가한다. 데이터는 이동 코드를 생성한 호스트의 공개키로 암호화되므로 이에 해당하는 비밀키를 갖는 호스트만 내용을 알 수 있다.

3.1.4 종단엔티티(End-Entity)

호스트는 이동 코드를 사용자의 원하는 목적에 따라 생성하여 원격지로 보낸다. 이때 자신의 인증을 위하여 전자 서명 값을 추가한다. 원격지에

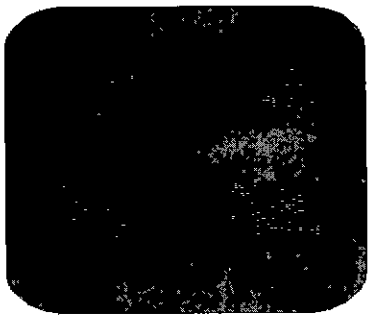


그림 7 이동 에이전트 코드

서 작업을 수행한 후 복귀한 에이전트는 그림 7에서와 같이 데이터와 추가 인증 정보가 함께 전달된다. 호스트는 추가 인증 정보에 대한 인증을 수행한 후 인증을 확인했을 경우 데이터를 자신의 비밀키로 복호화하여 원하는 데이터를 추출한다. 여러 원격서버를 거쳐서 생성된 데이터라 하더라도 각각은 호스트의 공개키로 암호화되었기 때문에 비밀키만 있으면 복호화를 할 수 있다. 또한 추가 인증 정보는 중간과정의 원격서버가 최종적으로 자신에게 전달한 인증 정보를 인증한 후 자신의 인증 정보를 기록하는 것이므로 이를 신뢰할 수 있다. 그러나, 최종 원격 서버에서 이전의 데이터를 모두 삭제한 후 자신의 데이터와 인증만을 추가하여 호스트로 보내질 위험이 있다. 이를 해결하기위하여 이동 코드내의 상태필드를 이용하는 방법을 다각도로 연구해야할 필요가 있다.

3.2 이동 코드 보안 관리 서버 및 호스트 모듈 개발

3.2.1 이동 코드 보안 관리 서버

이동 코드 보안 관리 서버의 목적은 호스트에서 생성한 에이전트를 보호함과 동시에 외부 침입자들의 이동 코드에 대한 불법적인 공격을 최소화하기 위함이 그 목적이다. 이러한 관리 서버는 각 호스트와 서버에 대한 권한 제어 리스트를 관리하고 적용하는 일을 담당한다. 즉, 이동 코드 내부에는 이동코드의 상태를 나타내는 상태 필드가 포함되어 있다. 이 상태 필드는 이동 코드의 다음 상태를 의미한다. 하나의 원격서버에서 작업을 수행한 후 다음 원격 서버로의 진행이나 또는 호스트로의 복귀들을 포함하는데 응용 서버에 위치한 이동 코드는 해당 서버로부터 이러한 상태의 전이를 허가해야 하므로 자칫 악용될 우려가 있다. 예를 들어, 항공사에 예약을 위한 이동 코드가 생성되어 원격서버를 방문했을 경우 A항공사 서버는 B사로 이동 코드를 전송하지 않고 자신의 데이터만을 탑재한 후 이동 코드의 상태를 호스트로 복귀하도록 변경하여 더 이상의 작업을 진행할 수 없도록 할 수 있다. 이러한 것을 막기 위해 권한제한을 사용하여 이동 코드의 상태를 전이할 경우 Agent Security Manager를 통해서만 가능하도록 하는 프로토콜을 설계한다. 또한 이동 코드의 창구를 일원화함으로 일관성 있는 통제를 수행할 수 있다는 장점을 가질 수 있다. 그러나, 이동 코드의 과부하로 인한 오버헤드 발생이 가능하므로 이에 대한 대책을 마련하여야 할 것이다.

3.2.2 호스트 모듈 개발

호스트에서는 이동 코드를 생성하여 작업을 부여한 후 원격 호스트로 전송한 후 작업을 마친 이동 코드로부터 데이터를 받아 원하는 결과를 이끌어낸다. 그러나, 여기서 주의할 점은 공개 네트워크를 통해 이동 코드가 불법적으로 변경되었거나 신뢰할 수 없는 데이터를 포함하는지의 여부를 판단해야 한다. 이동 코드를 통해 추가된 데이터는 호스트 자신의 공개키로 암호화되어 있으므로 자신의 비밀키로 복호화하여 이용한다. 이 데이터를 추가한 정보를 이동코드 내부에 상태필드로 확인 가능하며 Agent Security Manager를 통해 검증받을 수 있다. 또한 추가 서버 인증 정보는 이동 코드가 각 서버를 거치는 동안 연계적으로 인증된 정보이므로 최종적인 인증 정보만을 확인하면 된다.

이러한 인증 절차와 상태필드를 통해 이동 코드내의 데이터를 안전한 상태에서 이용할 수 있다.

3.3 이동 코드를 이용한 응용 프로그램

웹을 사용하는 사용자가 증가하면 할수록 현재의 상업적 행위가 온라인 상으로 옮겨가고 있는 추세이며, 앞으로도 계속 증가하게 될 것이다. 이러한 증가의 배경에는 전자 상거래가 전통적인 상거래보다 많은 이익을 주기 때문이다. 앞의 관

런 연구에서 보였듯이 에이전트 기술을 여러 응용 분야에 적용할 수 있으며, 특히 전자상거래 분야의 이동 에이전트 기술은 앞에서 보인 관련 연구에서 볼 수 있듯이 상점 검색, 가격 협상, 온라인 경매 등의 분야에 적용될 수 있다.

4. 결 론

근래에 인터넷의 발전으로 인해 수많은 사람들이 인터넷을 이용하고 있고 또한 이에 상응하는 전자상거래 쇼핑몰 등의 사업을 추진하고 있다. 이러한 사이트들에서 제공되는 서비스는 현재는 Interactive한 방법을 사용하여 사용자가 직접 방문하는 것을 원칙으로 하고 있지만 차후에는 이동 에이전트와 같은 이동 코드가 예약이나 쇼핑 등을 주도할 것으로 예상된다. 이에 시장 규모는 인터넷 사용자 전반에 걸쳐 이용될 수 있는 잠재력을 가졌다.

그러나, 이렇게 폭넓은 범위에서 사용될 수 있는 반면에 보안상의 취약점을 보완하지 않고서는 올바른 서비스를 지원하기가 어렵다. 앞에서 보인 예들처럼 전자상거래를 위한 여러 가지 시스템들이 연구되고 있지만, 아직까지는 보안상의 문제를 해결하려는 연구, 실험단계이며 실제적으로 상업적인 시스템 개발은 아직 이루어지지 않고 있는 실정이다. 따라서 본 연구에서 제안한 이동 코드 보안 시스템을 이용 사용자 인증과 권한제어 등의 메카니즘을 통해 보다 안전하고 신뢰할 수 있는 시스템을 구축한다면, 2003년경에 약 660억 달러로 예상되는 전자상거래 세계 시장의 조기 진출뿐만 아니라, 약 100억원 규모로 예상되는 국내 시장을 확보할 수 있을 것이다. 현재 국내에서는 공인된 인증기관으로 한국정보인증이라는 회사가 테동하여 인터넷 사이트에 인증서를 발급하고 있다. 이 공인된 인증기관의 인증서를 통하여 이동 코드의 인증을 수행하므로 인해 호스트의 사용자는 서비스를 받는 서버로의 인적사항이나 정보를 안심하고 전달할 수 있으므로 앞으로의 정보화 산업에 큰 영향을 미칠 수 있으리라 기대한다.

참고문헌

[1] RFC2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January, 1999.

[2] RFC2527, "Internet Public Key Infrastructure Certificate Policy and Cert ification Practies Framework", March, 1999.

[2] RFC2528, " Internet X.509 Public Key Infrastructure", March, 1999.

[3] "VeriSIgn", 1999, http:/www.verisign.com

[4] PKCS#10 v1.0, "Certification Request Syntax Standard", November, 1993

[5] "FIPA 98 specification", http://drogo.cselt.it/fipa/spec/fipa98/fipa98.htm, July, 1998.

[6] "Mobile Agent White Paper", General Magic, http://www.generalmagic.com/technology/techwhitepaper.html

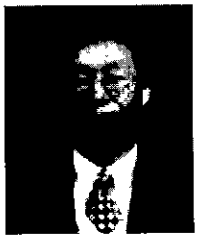
[7] McBride Baker & Coles, "Summary of Electronic Commerce and Digital Signature Legistration", http://www.mbc.com/legis/

[8] W.M. Farmer, J.D. Guttman, and V. Swarup. Security for Mobile Agents: Issues and Requirements. In Proc. of the 19th National Information Systems Security Conf., pages 591-597. Baltimore, MD, USA, October 1996.

[9] J. Tardo and L. Valente. Mobile agent security and Telescript. In IEEE Comp-Con, 1996.

[10] N. Karnik and A. Tripathi, "Design Issues in Mobile-Agent Programming Systems", IEEE Concurrency, Jul 1998.

원 유 헌



1972.2 성균관대 수학과 졸업(학사)
1975.8 한국과학기술원 전자계산학과(석사)
1985.8 고려대(이학박사)
1975~1976 한국과학기술연구소 연구원
1986~1987 R.P.I 객원 교수
1976~현재 홍익대학교 전자계산학과 교수
관심분야 : 컴파일러, 프로그래밍 언어 디자인, 소프트웨어 공학, 분산언어, 객체 지향언어, 하드웨어 기술언어, 이동 에이전트 보안 등.
E-mail : won@cs.hongik.ac.kr

2000년 논문지 편집회의일정

시스템 및 이론 : 홀수달 마지막주 금요일 16시
소프트웨어 및 응용: 짝수달 마지막주 금요일 (4, 10월 제외) 16시
데이터베이스 : 2, 5, 8, 11월 셋째주 수요일 16시
정보통신 : 2, 5, 8, 11월 넷째주 수요일 16시
위원장단회의 : 2, 5, 8, 11월 *표시한 날짜 15 - 16시

	시스템 및 이론	소프트웨어 및 응용	데이타베이스	정보통신
1월	28(금)			
2월		25(금)	*16(수)	23(수)
3월	24(금)			
4월		21(금)		
5월	26(금)		17(수)	*24(수)
6월		30(금)		
7월	28(금)			
8월		*25(금)	16(수)	23(수)
9월	29(금)			
10월		20(금)		
11월	*24(금)		15(수)	23(수)
12월		29(금)		

※ 회의일정은 사정에 따라 변경될 수 있음.