韓國 컴퓨터情報學會 論文誌
第9卷 第3號, 2004. 9.

2004-9-3-3-6

강하고 안전한 이동 에이전트 시스템을 위한 게이트웨이 설계에 관한 연구

김 효 남*

A Study on the Design of the Gateway for a Strong and Safe Mobile Agent System

Hyo-Nam Kim*

요 약

최근 인터넷 환경 속에서 네트워크와 관련된 많은 기술들이 연구되어 왔다. 이 중 네트워크 기반에서 적용할 주문형태의 기능을 제공하는 방법으로 이동 에이전트에 대한 연구가 폭넓은 관심을 가지게 되었다. 그러나 유해 침입에 대한 잠재성, 정보 유출과 같은 자원의 악용, 그리고 다른 여러 가지 보안상의 문제들로 인해 커다란 장애를 받고 있다. 그래서 이동 에이전트는 획기적인 패러다임으로 여기고 있으나 보안상 많은 취약점을 가지고 있다. 본 논문에서는 이동 에이전트 시스템과 그 자체에 대한 보안을 강화시킬 수 있는 방법으로 보안 정책 데이터베이스를 가지고 에이전트 코드를 분할하고 합병하는 기술로 이동에이전트의 취약점을 해결하기 위한 방안을 제시할 수 있는 강하고 안전한 이동 에이전트 시스템의 게이트웨이 설계를 제안하였다.

Abstract

In the course of Internet proliferation, many network-related technologies are examined for possible growth and evolution. The use of Internet-based technologies in private networks has further fuelled the demand for network-based applications. The most promising among the new paradigms is use of mobile agents. It also however, suffers from a major drawback, namely, the potential for malicious attacks, abuse of resources pilfering of information, and other security issues. These issues are significantly hampering the acceptance of the mobile-agent paradigm. This paper proposed the design of strong and safe mobile agent gateway that split and merge the agent code with security policy database. This mechanism will promote the security in mobile agent systems and mobile agent itself.

▸ Keyword : MASG(Mobile Agent Gateway), SPD(Security Policy Database), ATP(Agent Transfer Protocol), IPSec(Internet Protocol Security)

• 제1저자 : 김효남
• 접수일 : 2004.08.21, 심사완료일 : 2004.09.03
* 청강문화산업대학 컴퓨터소프트웨어과

Ⅰ. 서 론

최근 인터넷 환경 속에서 네트워크와 관련된 많은 기술들이 연구되어 왔다[3][4]. 이 중 클라이언트가 적용할 주문형태의 기능을 제공하는 방법으로 이동 에이전트에 대한 연구가 폭넓은 관심을 가지게 되었다. 이동 에이전트는 임의의 호스트로부터 다른 호스트를 이동하며 사용자의 역할을 대신 수행하는 프로그램이다. 이동 에이전트는 코드, 상태 변수 그리고 다음 이동지의 리스트를 나타내는 여정리스트로 구성되어져 있다. 코드는 에이전트가 수행되는 동안 변경되지 않는 반면에 상태변수는 이동 에이전트가 수행되는 동안 변경된다. 이동 에이전트는 클라이언트의 요구를 수용할 수 있는 기능과 프로그램 내부에 소프트웨어 모듈들을 통합하여 이동할 수 있다는 장점을 통해 부각되기 시작했다. 이는 서로 다른 분산 환경에서 사용자의 역할을 대신하여 특정한 작업을 수행할 수 있다는 것이다. 이동 에이전트는 우선 사용자의 기계에 위치한 후 수행을 위해 원격지로 보내지게 된다. 호의적인 호스트들은 이동 에이전트가 수행하기 위한 적절한 환경을 제공한다. 이를 이동 에이전트 플랫폼이라 한다. 이동 에이전트는 이동 후 호스트 내에서 수행되어 정보를 수집하고 다음 여행지로 이동하기 위하여 자체적으로 상태와 변수들을 실시간적으로 수정한다. 이러한 여행을 마지막 호스트까지 수행한 후 자신의 홈으로 귀환한다. (그림 1)은 이러한 이동에이전트의 동작 및 이동 에이전트 시스템에 대한 조직도를 나타내고 있다[5][7].

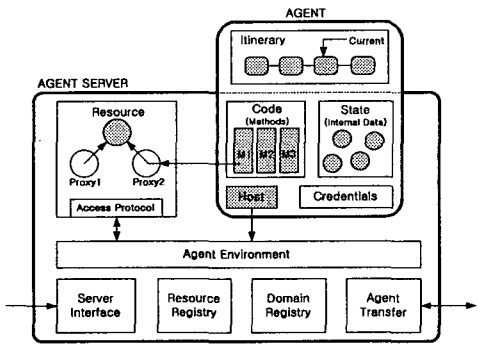

그림 1. 이동 에이전트 시스템 구성

그러나 이동 에이전트는 자율성, 적응성, 이동성과 같은 특성으로 인해 획기적인 패러다임으로 여겨졌으나 보안상 많은 취약점을 가지고 있다. 즉, 이동 에이전트를 통한 호스트에 대한 보안과 호스트에 의한 이동 에이전트에 대한 보안, 또한 이동 에이전트간의 정보 교환 시 발생할 수 있는 이동 에이전트 간에 대한 보안등이다. 예를 들어 네트워크를 이동하는 이동 에이전트에 대한 신뢰성과 보안성에 대한 관심이 일어났다. 즉, 이동 에이전트가 어떠한 유해한 방해나 공격 없이 수행할 수 있을 것인가 하는 의문이 제기되었다[1][2].

본 논문에서는 이동 에이전트의 취약점 가운데 이동 에이전트가 불법적인 호스트를 통해 공격을 당할 수 있는 위험성을 분석하고 이를 해결하기 위한 방안에 대해 해결책을 제시할 수 있는 이동 에이전트 게이트웨이 시스템 설계를 제안한다.

Ⅱ. 관련 연구 분석

2.1 분리되지 않는 서명(Undetachable Signatures)

분리되지 않는 서명 방법은 Sander와 Tschudin에 의해 제안되었다[6]. 그리고 이는 CEF (*Computing with* Encrypted Function)라 불리는 방법에 기초를 두고 있다. 여기서 이동 에이전트는 s를 자신의 서명 함수로 대동하며 호스트는 이 함수를 통해 호스트의 결정을 서명하게 된다. 그러나 이 서명 함수는 호스트에게 드러나게 되므로 이를 암호화된 함수 f을 통해 암호화하여 s를 참조하는 대신 $s \circ f$를 이용하여 일을 처리하게 한다. 예를 들어 소비자는 인터넷을 통하여 물건을 구매하기 위하여 이동 에이전트를 보내고자 한다고 가정하자. 이때 소비자의 서명 함수 s를 사용할 수 있을 경우만 에이전트는 트랜젝션을 인증한다. 그러나 에이전트는 잠정적으로 유해한 호스트에서 수행될 수 있다. 따라서 이 s를 보호하기 위하여 다음과 같은 암호화 함수를 이용하여 호스트는 s를 직접적으로 알 수 없게 한다.

$f_{signed} = s \circ f$ (1) - 암호화된 함수를 통해서만 서명 함수를 접근가능(s : 서명 함수, f : 암호화된 함수, o : 함수 결합)

이러한 암호학적인 방법을 통해 에이전트의 보안성을 개선시켰다. [그림 2]는 RSA 알고리즘을 이용한 전체적인 구조를 나타내고 있다. 즉, 이동 에이전트의 역할을 수행하고 난 후 그에 해당하는 데이터를 호스트에서 제공하게 된다. 이때 이 데이터는 평문형태로 부여되는 것이 아니라 서명을 통해서만 접근하겠다는 방법이다. 또한 서명함수를 이용할 때 이동 에이전트가 제시하는 암호화된 함수를 통해서만 서명이 가능하므로 직접적으로 서명을 할 수 없으므로 데이터 값의 변경이 불가능하다는 장점을 지닌다. 그러나 이러한 암호화된 서명을 통한 방법은 이동 에이전트의 여정리스트를 변경하거나 또는 암호 모듈을 전체적으로 다른 암호 모듈로 대체하였을 경우의 단점이 드러나게 된다. 또한 모든 데이터를 암호화할 수 없으므로 인해 보안상의 문제가 여전히 남아 있게 된다.

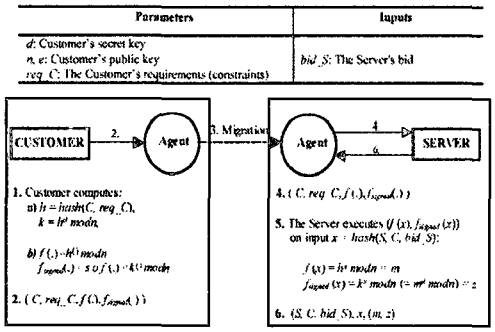

그림 2. RSA를 이용한 안전한 서명 스키마

2.2 스마트카드를 이용한 에이전트 보호

에이전트의 보호를 위하여 스마트카드를 이용하는 방법이 제안되었다[8]. 이 방법은 에이전트의 보호를 위해 에이전트에 대한 모든 참조 및 연산 등을 컴퓨터상에서 수행하지 않고 스마트카드 내부에서 수행한다. 예를 들어 자바카드와 같은 신뢰할 수 있는 카드를 이용하여 다음과 같은 기능에 따라 수행된다.

- 암호화된 코드 부분을 입력받는다.
- 카드 내에서 데이터를 복호화하고 수행되는 경로상에 데이터를 저장한 후 수행한다.
- 다음 이동될 카드의 키를 이용하여 결과를 암호화한 후 에이전트에게 전송한다.

[그림 3]은 이러한 스마트카드 내부의 구조를 나타내고 있다. 스마트카드를 이용할 경우 외부로 복호화 된 데이터가 드러나지 않으므로 신뢰성 있는 에이전트 수행을 기대할 수 있다. 또한 다른 하드웨어 장비에 비해 저렴한 가격과 보편화되어 있다는 장점을 가진다. 그러나 이러한 스마트카드를 이용하는 방법은 다른 스마트카드간의 상호적인 키를 알아야 하므로 중앙 집중적인 방법을 통해 관리를 해야 하고 또한 모든 관계된 키를 추가 변경이 생길 때마다 갱신해야 하는 번거로움이 있다. 또한 하드웨어의 처리 능력이 다소 떨어지므로 고속연산이나 큰 데이터를 처리하는 데는 다소 문제가 있다고 할 수 있다.

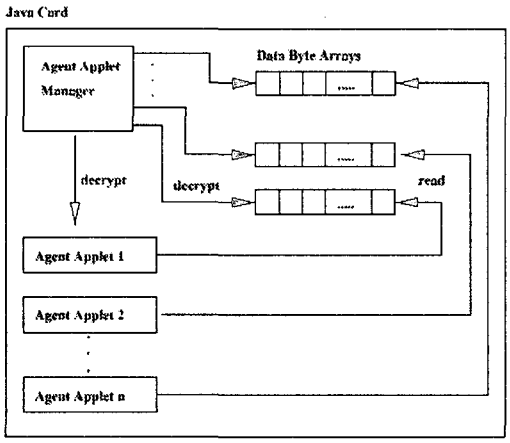

그림 3. 스마트카드의 구조

III. 이동 에이전트 게이트웨이(MAG)의 설계

이동 에이전트 보안에 대해 제시된 이론들은 이동 에이전트에 대한 공격을 줄일 수는 있으나 완벽하게 보안을 달성할 수 있는 방안은 아니다. 또한 코드상으로 많은 오버헤드를 감수해야만 한다. 현실 세계에서 다수의 사용자가 호스트를 이용할 경우 호스트에 과중한 부하가 생길 수도 있다. 이 논문에서는 이러한 단점들을 보완하기 위하여 이동 에이전트와 이동 에이전트 시스템 이외에 추가적인 개체로 이동 에이전트 게이트웨이 시스템을 제안하고자 한다.

3.1 이동 에이전트 게이트웨이 시스템

MAG은 내부망을 보호하기 위하여 내부망의 게이트웨이 역할을 수행하며 또한 암/복호화를 지원하기 위해 암호 모

들을 탑재하였다. MAG 시스템에서 필요한 구성 요소를 다음과 같이 정의한다.

- 클라이언트 : 이동 에이전트를 생성하여 이를 통해 사용자의 역할을 대신 수행하고자 하는 사용자 또는 시스템
- 에이전트 풀 : MAG을 통해 전송된 원본 이동 에이전트를 일시적으로 보관하는 데이터베이스로 에이전트의 분할 및 병합에 사용
- 보안정책(SPD-Security Policy Database) : 보안 정책 데이터베이스로 이동 에이전트에 적용할 규칙들을 저장하는 데이터베이스
- 관리 시스템 : 보안정책 및 에이전트 풀 및 MAG등을 관리하는 전체적인 운영/관리 시스템
- 호스트 : 이동 에이전트를 전송 받아 수행시키며 이동 에이전트의 역할에 대해 응답해주는 일종의 서버 시스템

(그림 4)는 MAG의 전체적인 시스템의 구성도를 나타내고 있다[9].

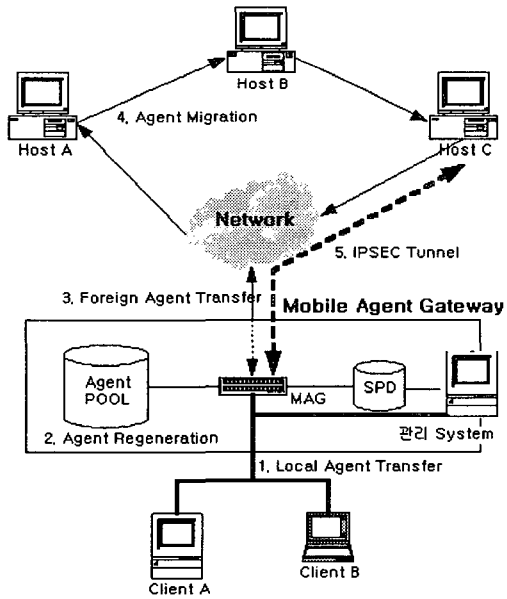

그림 4. 이동 에이전트 게이트웨이

3.2 MAG의 구조

이동 에이전트는 이동 에이전트 시스템에서 수행하는 동안 코드를 통해 호스트의 자원을 참조한다. 이동 에이전트는 목표한 결과를 얻었을 경우 내부적으로 상태를 변경시킨 후 여정리스트에 따라 다음 목적지로 이동한다. 이때 ATP(Agent Transfer Protocol)를 통해 다음 호스트로 전송된다. 이러한 환경 속에서 만약 호스트가 불법적으로 상태를 변경하거나 여행 목적지를 강제로 변경할 경우가 발생할 수 있다. 또한 내부 데이터 중에서 민감한 데이터가 포함되어 있을 경우 문제는 더욱 심각해진다. 따라서 MAG에서는 이러한 단점을 보완하기 위하여 에이전트를 안전한 최소단위로 분할하고 민감한 데이터를 제거하여 호스트로 전송한다. (그림 5)는 이동 에이전트 게이트웨이의 내부구조를 나타내고 있다.

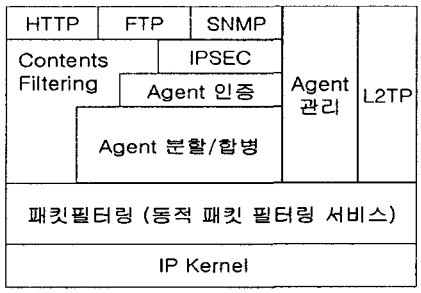

그림 5. 구현된 MAG의 내부구조

3.3 MAG에서의 에이전트 처리과정

(그림 6)은 MAG의 구성요소별 상관관계에 대해 나타내고 있다. 이동 에이전트는 사용자의 PC를 떠나 이동 에이전트 게이트웨이에 도착하게 되고 (그림 5)와 (그림 6)의 구조에 따라 이동 에이전트를 처리하게 된다.

다음은 이동 에이전트 게이트웨이에서 에이전트를 처리하는 과정을 기술한다.

- 클라이언트로부터 전송된 에이전트에 대해 인증을 수행
- 에이전트 내의 클래스 정보에 따라 보안정책을 적용
- 적용된 보안정책에 따라 여정리스트를 분할하여 에이전트 재구성
- 에이전트의 클래스에 따라 데이터 내부에 정보를 에이전트 풀에 에이전트와 함께 저장
- 재 생성된 이동 에이전트에 인증정보와 IPSec정보를 추가하여 호스트로 전송

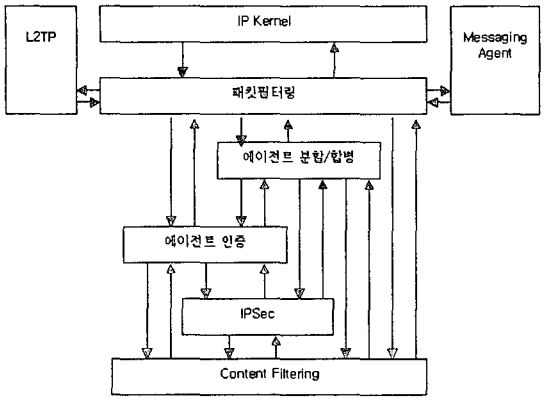

그림 6. MAG의 구성요소별 상관관계

위의 과정을 거친 이동 에이전트는 호스트에 도착한 후 IPSec정보를 통해 MAG과 통신을 수행하게 된다. 이때 에이전트 풀에 저장된 데이터를 안전하게 호스트로 전송하게 되며 호스트 또한 에이전트에게 부여할 결과 데이터를 MAG으로 보내게 된다. 이동 에이전트는 MAG으로 귀환한 후 에이전트 풀에 있는 원본 에이전트의 내용을 토대로 다시 합병을 수행한다. 합병을 마친 후 MAG은 호스트로부터 전송 받은 결과 데이터를 에이전트 데이터에 첨가하고 다시 서명한 후 클라이언트에게 전송한다.

3.4 MAG의 구성요소별 세부기능

패킷필터링에서는 정해진 규칙에 따라 수신된 패킷을 필터링하는 기능을 수행한다. IP 커널을 거친 모든 패킷은 특정한 패킷(Broadcasting 패킷, Non-IP packet 등)을 제외하고는 모두 패킷필터링을 거치게 된다. 여기에서 특정한 패킷은 수신한 직후에 바로 미리 설정된 설정 사항에 따라 바이패스를 시킬 것인지, 또는 버릴 것인지를 결정한다. 패킷필터링에서는 정해진 규칙에 따라 패킷을 필터링하는 일반적인 필터링 부분과, 정해진 규칙으로부터 파생된 부가적인 규칙을 이용하여 동적으로 패킷을 필터링 할 수 있는 동적 패킷필터링이 있다. 이러한 패킷 필터링 기능을 이용하여 이동 에이전트에 대한 필터링을 수행한다.

에이전트 코드 분할/합병에서는 클라이언트로부터 이동 에이전트를 수신한 후 분석기를 통해 원본 코드를 분류한다. 구분된 코드는 보안정책상에 클라이언트의 정책에 따라 재구성된다. 이러한 정책은 관리자에 의해 설정 가능한 정보로 유지한다. 이 과정을 통해 보안정책상에 외부로 유출을 금지한 코드를 포함하였을 경우 코드 상에서 제외되고 안전한 코드만을 이용하여 이동 에이전트는 재구성된다. 원본 코드는 마지막 결정을 위해 에이전트 풀에 위치시킨다. 또한 코드를 재구성할 때 여정리스트를 보안정책 리스트에서 검사하여 위험한 호스트로 등록이 되어있을 경우 이를 분할한다. 즉, 위험 가능성이 있는 호스트일 경우는 다른 호스트와의 연계성을 배제함으로 인해 보다 안전한 통신을 하기 위함이다. 이러한 불법적인 호스트의 등록은 테스트 이동 에이전트를 통해 점진적으로 구축해 나간다. 이렇게 재구성되고 분할된 이동 에이전트는 외부 호스트로 이동되어 작업을 수행한다. 이동 에이전트 인증은 망을 사용하는 대부분의 패킷에 대해 IP 주소를 기반으로 통신을 제어하던 기존 방식과 달리 사용자 인증서 즉, PKI를 기반으로 통신을 제어하는 기능이다. 사용자는 자신의 인증서를 이동 에이전트에 일임함으로 인해 이동 에이전트가 대리인의 역할을 함과 동시에 전자서명의 특성을 가질 수 있도록 인증서 기반의 인증을 수행한다. 인증서는 X.509에서 지정한 표준 인증서를 준용한다. 따라서 이동 에이전트의 코드에는 다음의 형식과 같은 메시지 형식을 따른다.

Mobile Agent Code	signClient

IPSec(Internet Protocol Security)은 TCP/IP 프로토콜의 구조적인 결함을 극복하고 IP 수준에서 제공되는 보안 서비스를 표준화할 목적으로 개발된 인터넷 보안 표준이다. 이동 에이전트에서는 통신 데이터의 비밀성과 무결성 등을 보장하기 위하여 IPSec 기능의 암복호화 기능을 이용하여 외부의 호스트로 전송된 후 데이터에 대한 송수신을 IPSec을 통하여 이동 에이전트 게이트웨이와 수행한다. 이때 송/수신되는 정보는 이동 에이전트가 호스트에게 제공해야하는 민감 데이터와 호스트로부터 이동 에이전트에게 전송할 결과데이터를 암/복호화여 호스트와 MAG 사이에 진행된다. 이 논문에서는 IPSec을 이용한 암호화 프로토콜을 사용하였으나 SSL과 같은 프로토콜로 변형하여도 가능할 수 있다.

Ⅳ. 결론 및 향후 계획

기존의 분산 환경에서 대두된 이동 에이전트는 불법적인 호스트들에 대한 위험성 때문에 실제 응용에 적용하는데

많은 문제점이 있었다. 본 논문에서는 안전한 제3의 개체인 MAG을 통해 이러한 이동 에이전트의 보안상의 문제점을 해결하였고 그에 따른 부담을 클라이언트에게는 투명하게 유지하였다. 따라서 불법적인 호스트로부터 클라이언트의 이동 에이전트를 안전하게 유지할 뿐만 아니라 코드를 재생성함으로 인해 보다 민감한 데이터를 유출하는 것으로부터 막을 수 있다. 이는 현재 가장 많이 네트워크 상에서 사용되는 VPN 장비 등을 이용하여 구축함으로 인해 시설 추가에 따른 부담을 줄일 수 있다. 하지만, 제3의 개체를 더 경유해야하는 추가 부담으로 인한 오버헤드는 여전히 문제점으로 남고 있다. 이를 좀 더 개선하기 위한 방안이 필요하겠다.

또한 보안정책에 대한 점진적이고 적응적인 구축이 더 연구되어야하며 제3의 매체인 MAG의 처리능력에 따라 이동 에이전트 시스템뿐만 아니라 이를 게이트웨이로 이용하는 내부망 전체 시스템에도 막대한 영향을 초래할 수 있다는 점에서 MAG의 성능 개선은 필수 사항이라 하겠다. 결과에서도 알 수 있듯이 상호인증을 위한 인증서 기반의 서명 검증 등의 공개키 연산이 필수적이여서 MAG 시스템에 공개키 가속기 등을 설치하는 방안도 검토해야 할 것이다. 하지만, 무엇보다도 이러한 이동 에이전트 자체에 대한 보안성에 대한 이론적 정립이 미흡하고 해결방안이나 테스트에 대한 인지도가 낮다는 현실도 간과해서는 안 될 것이다.

참고문헌

[1] Hyo-Nam Kim, "A Study on the Design of Intruder Tracing System Using Intrusion Method", 2003. 9, 韓國 컴퓨터情報學會 論文誌 第8券 第3號

[2] Hyo-Nam Kim, "An Efficient Algorithm for Detecting Stepping Stones", 2002. 3, 韓國 컴퓨터情報學會 論文誌 第 7券 第1號

[3] D.C, Chess, C. Harrison, A. Kershen- baum, "Mobile Agents:Are They a Good Idea?", IBM Research Report, 1995.

[4] R. S. Gray, "Agent Tcl: A flexible and secure mobile-agent system", Procee- dings of Fourth Annual Usenix Tcl", Workshop, pp.9-23, 1996

[5] Crystaliz Inc., General Magic Inc., GMD Fokus, IBM Corp., "Mobile Agent Facility Specipication", Joint Submission Sup- ported by the Open Group, OMG TC Document, November 1997.

[6] Hartmut Vogler, Thomas Kunkelmann, Marie-Louise Moschgath, "An Approach for Mobile Agent Security and Fault Tolerance using Distributed Transact- ions", Proceedings of the 1997 Inter- national Conference on Parallel and Distributed Systems, pp.268-274,1997 IEEE.

[7] F. Hohl, "A model of Attacks of Malic- ious Hosts Against Mobile Agents", presented at 4th Workshop on Mobile Object Systems" Secure Internet Mobile Computations, France, 1998.

[8] Stefan Funfrocken, "Protecting Mobile Web-Commerce Agents with Smartcard", Mobile Security Agent, LNCS 1419, 1999, springer, pp.44-64, Giovanni Vigna (Ed.)

[9] Jae-Kyoung Park, Yoo-Hun Won, "Protecting Mobile Agent with VPN", 2001. 6, 情報保護學會 論文誌 第 11券 第3號

저 자 소 개

김 효 남

1988년 홍익대학교 전자계산학과 (이공학사)

1990년 홍익대학교 전자계산학과 (이공석사)

2002년 홍익대학교 전자계산학과 박사수료

현 재 청강문화산업대학 컴퓨터소프트웨어과 부교수

〈관신분야〉 Programming Language, Object Oriented Programming, 컴퓨터 보안