제26회 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호 (2006. 11)

전자 상거래 환경에서 이동 에이전트의 데이터 보호 기법*

정용우, 조현진, 김구수, 엄영익
성균관대학교 정보통신공학부
e-mail:{withdubu, hjcho, gusukim, yieom}@ece.skku.ac.kr

Protection of Mobile Agent Status in e-Commerce Environments

Young Woo Jung, Hyun-jin Cho, Gu Su Kim, and Young Ik Eom
School of Information and Communication, Sungkyunkwan University

요 약

전자상거래 환경에서 이동 에이전트는 사용자의 요구 사항을 바탕으로 사용자가 원하는 상품을 검색, 협상, 구매의사 결정 등을 하는 자율적인 프로그램을 말한다. 이동 에이전트를 사용함으로써 나타나는 많은 장점에도 불구하고 이동 에이전트가 갖는 자체적인 보안 위협으로 인해 전자상거래 환경에 적용하는데 어려움이 있다. 특히 이동 에이전트가 저장하고 있는 정보에 대한 위변조 위협은 사용자로 하여금 정확한 상품 구매를 방해하는 중요한 문제이다. 본 논문에서는 공유키 암호화 기법과 공개키 암호화 기법을 이용한 키 교환 메커니즘을 통해 이동 에이전트 내부에 저장된 정보를 보호하는 기법을 제안한다.

1. 서론

인터넷의 빠른 보급과 통신망의 고속화에 기초하여 전자상거래(Electronic Commerce)는 새로운 비즈니스 모델로 자리 잡았다. 전자상거래란 사람과 사람이 물리적인 매체의 전달을 통해 상품을 사고파는 전통적인 상거래와는 달리 컴퓨터와 네트워크라는 전자적인 매체를 통해 상품을 거래하는 행위를 말한다. 전자상거래 환경은 다양한 상품에 대한 빠른 구매 의사 결정을 통해 판매자와 소비자 모두의 요구를 만족 시킨다. 이러한 전자상거래 환경에서의 이동 에이전트의 도입은 사용자로 하여금 보다 효과적인 상품의 거래를 가능하게 한다[1, 2].

이동 에이전트(Mobile agent)는 네트워크를 이동하며 사용자를 대신하여 주어진 작업을 수행하는 프로그램을 말한다[3]. 이동 에이전트는 동일한 에이전트를 복제해 다수의 서버로 보내고 이후에 그들이 가져온 데이터를 모아 복합적인 결과를 만들어내는 특징을 가진다[4]. 이러한 이동 에이전트의 특징은 전자상거래에서 유용하게 사용될 수 있다.

전자상거래 환경에서 상품에 대한 정보는 정형화되지 않은 형태로 분산되어 존재한다. 이동 에이전트의 이동성(mobility)은 분산된 상품에 대해 효과적인 검색을 가능하게 한다[5]. 뿐만 아니라 실제적인 거래에 대한 자율성을 부여함으로서 사용자의 요구에 맞는 상품을 구매할 수 있다[6].

이러한 장점에도 불구하고 이동 에이전트가 갖는 자체적인 보안 취약성으로 인해 실제 전자상거래에 도입하기에는 어려움이 있다. 이동 에이전트는 상품 구매 과정에서 필요한 구매정보, 결제정보, 배송정보 및 상품 검색 등의 작업을 통해 얻은 메타 데이터(meta data)를 내부에 저장한다. 이 정보들은 네트워크를 통한 이주 과정에서 외부 공격자의 위변조 위협에 노출될 수 있다. 본 논문에서는 이러한 위협으로부터 이동 에이전트의 정보를 보호하기 위한 메커니즘을 제안한다. 본 논문은 다음과 같이 구성된다. 2장에서는 이동 에이전트 시스템 보안 모델을 살펴보고 3장에서는 이동 에이전트를 이용한 전자상거래에서의 보안 위협 요소를 기술한다. 4장에서는 이동 에이전트의 정보를 보호하기 위한 메커니즘을 제시하고 5장에서 결론을 맺는다.

* 본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업의 지원에 의한 것임 (2006-0391-0100).

2. 이동 에이전트 시스템 보안 모델

2.1 Aglets

IBM에서 만들어진 Aglets[7]는 서로 신뢰 할 수 있는 호스트로 구성된 네트워크를 가정한다. Aglets는 프락시(Proxy) 객체를 이용하여 이동 에이전트와 호스트를 보호하는 방법을 사용한다. 이동 에이전트는 프락시를 통해 호스트에 접근 한다. 프락시는 이동 에이전트에게 허락된 자원에만 접근 할 수 있도록 하는 통로의 역할을 한다. 따라서 이동 에이전트는 프락시를 통하여 접근 가능한 자원만 이용할 수 있다.

Aglets는 이동 에이전트가 직접 이동 에이전트 시스템의 자원의 접근 할 수 없기 때문에 이동 에이전트로부터 시스템의 자원을 안전하게 보호 할 수 있다. 또한 이동 에이전트의 요청에 의해 프락시가 생성됨으로써 시스템의 주원을 절약할 수 있다. 뿐만 아니라 프락시는 이동 에이전트에게 안전한 상태에서 호스트로부터 서비스를 받을 수 있는 환경을 제공함으로서 이동 에이전트를 보호한다.

2.2 Ajanta

Ajanta[8]는 자바를 기반으로 만들어진 이동 에이전트 시스템이다. Aglets와 마찬가지로 프락시 객체를 이용하여 시스템 자원에 대한 이동 에이전트의 직접적인 접근을 제한한다. 또한 Ajanta는 이동 에이전트에게 신임장(Credential)을 발급하여 자원의 접근 법위를 결정함으로서 시스템 자원을 보호한다.

Ajanta는 이동 에이전트에게 읽기 전용 상태(Read only state)와 추가 전용 상태(Append only State)를 정의한다. 이러한 접근 모드는 이동 에이전트가 가지고 있는 정보를 보호한다.

3. 보안 위협 요소

3.1 전자상거래에서 호스트 보안 위협요소

이동 에이전트는 상품을 판매하는 호스트에 대한 공격의 주체가 될 수 있다. 이동 에이전트는 호스트의 상품 내용이나 가격 등의 정보를 변경함으로써 시스템에 악영향을 준다. 표 1은 이동 에이전트가 호스트에 가할 수 있는 대표적인 위협 요소 이다.

<표 1> 호스트의 보안 위협 요소

보안 위협 요소
- 시스템 파괴 및 마비
- 상품 내용, 가격 등의 상품 정보 변경
- 제품의 평가 자료 변경
- 고객 정보의 유출 및 변경
- 시스템 서비스 거부 공격

3.2 전자상거래에서 이동 에이전트 보안 위협요소

이동 에이전트는 상품 구매에 필요한 다양한 정보와 작업을 통해 얻은 메타 데이터를 내부에 저장한다. 신뢰할 수 없는 호스트나 외부의 공격자는 이동 에이전트에 저장된 정보를 유출 또는 변경함으로써 올바른 상품 구매를 방해한다. 표 2는 상품 구매 과정에서 나타날 수 있는 단계별 보안 위협 요소이다.

<표 2> 이동 에이전트의 보안 위협 요소

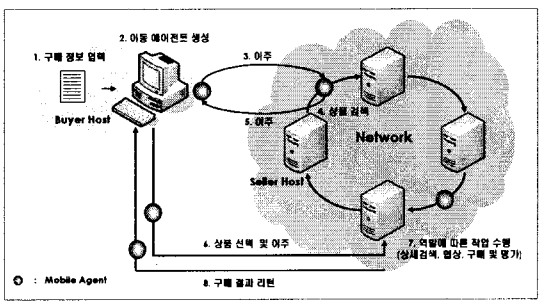
단 계	위협 요소
상품 검색	수집된 상품 정보의 변경 및 유출
상품 선택	사용자의 요구 사항 변경 이동 에이전트의 구매 정책 변경
협상 단계	협상 정책 및 처리 절차 변경 잘못된 협상 결과 유도
결제 및 배송	신용카드 번호 및 암호 유출 전자 화폐의 이중 사용 지불 내용 변경 및 삭제 배송 정보 변경
서비스 및 평가	자율적 평가 방해 및 내용 변경

전자 상거래 환경에서 이동 에이전트에 대한 공격의 핵심은 이동 에이전트가 가지고 있는 정보 및 데이터의 위변조이다. 본 논문에서는 공유키 암호화 기법과 공개키 암호화 기법[9]을 이용한 키 교환 메커니즘[8]을 통해 이동 에이전트 내부에 저장된 데이터를 안전하게 보호 할 수 있는 기법을 제안한다.

4. 이동 에이전트의 데이터 보호기법

4.1 이동 에이전트를 이용한 전자상거래 모델

전자상거래 환경에서 이동 에이전트는 사용자의 요구 사항을 바탕으로 사용자가 원하는 상품을 구매하기 위해 필요한 작업을 수행하는 자율적인 프로그램이다. 그림 1은 이동 에이전트를 이용한 전자상거래 환경을 나타낸다.



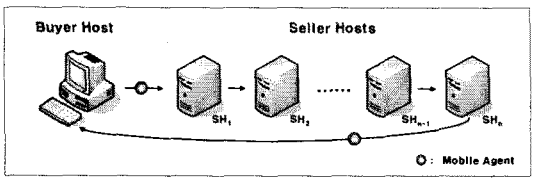
(그림 1) 이동 에이전트를 이용한 전자상거래 환경

각 Seller Host는 TTP(Trusted Third Party)로서 서로를 충분히 신뢰할 수 있으며 공유키(Shared Key)를 가지고 있다고 가정한다.

Buyer Host는 사용자의 요구사항을 입력받아 이동 에이전트를 생성한다. 이동 에이전트는 네트워크를 이동하며 사용자의 요구 사항에 부합하는 상품을 검색 한 뒤 돌아온다. 사용자는 Buyer Host로 돌아온 이동 에이전트의 검색 결과를 바탕으로 관심 있는 상품을 선택한다. 이동 에이전트는 사용자가 선택한 상품을 취급하는 Seller Host로 이동하여 협상, 결제 및 배송 과정을 거친다. 성공적으로 구매가 완료되면 이동 에이전트는 Buyer Host로 돌아와 사용자에게 구매 결과를 보고 한다.

4.2 상품 검색 메커니즘

이동 에이전트는 사용자가 원하는 상품을 검색하기 위해 그림 2와 같이 다수의 Seller Host를 이동하며 검색 결과를 취합한다.



(그림 2) 이동 에이전트의 상품 검색

이 과정에서 이동 에이전트가 수집한 상품 정보는 신뢰할 수 없는 호스트나 다른 외부의 공격자에게 노출되어 변경 되거나 삭제 될 수 있다. 이를 방지하지 하기 위해 각각의 Seller Host를 통해 수집된 상품 정보는 Buyer Host의 공개키로 암호화되어 이동 에이전트에 저장된다. 그림 3은 이동 에이전트에 저장된 상품 검색 결과를 보인다.

$$SR_{tot} = \sum_{k=1}^{n} E_{KU_{BH}} (IG_{SH_k} \mid SHID_{SH_k} \mid RK_{SH_k} \mid H(IG_{SH_k} \mid SHID_{SH_k} \mid RK_{SH_k}))$$

(그림 3) 이동 에이전트에 저장된 상품 검색 결과

검색결과(SR)는 검색된 관심대상 품목(IG)과 Seller Host ID(SHID), Seller Host에서 생성한 Random Key(RK) 그리고 앞의 값들의 무결성을 검사하기 위해 해쉬 함수를 적용한 영역으로 구성된다. RK는 메시지 교환을 통해 Seller Host와 Buyer Host간에 공유된다. 이동 에이전트에 의해 수집된 상품 정보는 그림 3과 같은 메시지 형식으로 공격자의 위변조의 위협으로부터 안전하게 Buyer Host로 전달된다.

4.3 상품 선택 메커니즘

사용자는 이동 에이전트에 의해 수집된 검색결과를 복호화 하여 구매하고자하는 상품을 선택한다. 이동 에이전트는 사용자가 구매하고자 하는 관심 품목을 Seller Host에게 전달한다. 그림 4는 Seller Host에게 전달되는 관심 품목에 대한 메시지 구조를 나타낸다.

$$SG = E_{RK_{SH_k}}(IG_{SH_k} \mid MAID \mid H(IG_{SH_k} \mid SHID_{SH_k} \mid MAID))$$

(그림 4) 관심 품목 메시지 구조

관심 품목 메시지(SG)는 해당 호스트에서 검색된 관심 품목(IG)과 검색을 담당한 이동 에이전트 ID (MAID), 그리고 무결성 검사를 위해 해쉬함수를 적용한 영역으로 구성된다. 이 메시지는 상품 검색 단계에서 Seller Host에 의해 발급된 RK에 의해 암호화된다.

Seller Host는 이동 에이전트로부터 메시지를 넘겨받아 무결성을 검사하고 사용자가 선택한 상품 정보를 확인한다. 그림 5는 상품 선택 메커니즘을 보인다.

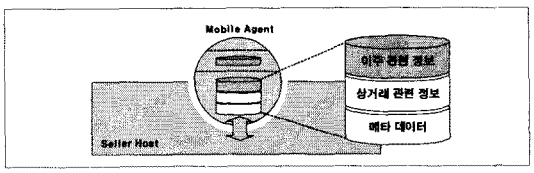
```
getInterestedGoods(SG, shid){
        sg    = D_RK(SG);          // 공유키 RK를 이용하여 복호화
        ig    = getIG(sg);         // get IG
        maid  = getMAID(sg);       // get MAID

        a     = getHash(sg);       // get H(IG, SHID, MAID)
        b     = H(ig, shid, maid);
        if (a=b)                   // 무결성 검사
              Negotiation(ig, ···)
        else
              Refuse(···)
}
```

(그림 5) 상품 선택 메커니즘

4.4 이동 에이전트의 내부 정보 보호

이동 에이전트는 호스트간의 이주를 통해 수집한 메타 데이터 외에 자신이 생성되는 시점에서 홈 플랫폼으로부터 부여받은 정보를 저장 한다. 이 정보는 이주 관련 정보와 상거래 관련 정보로 나뉜다. 그림 6은 이동 에이전트에 저장된 정보를 나타낸다.



(그림 6) 이동 에이전트에 저장된 정보 분류

이주 관련 정보는 이주할 Seller Host 주소, 홈 플랫폼의 ID 등의 이주에 필요한 정보로써 이동 에이전트 생성 시점에 플랫폼으로부터 이동 에이전트에 적재 된다. 이주 관련 정보는 이동 에이전트의 상거래 행위에 직접적으로 관여하지 않는다. 따라서 Seller Host에게 전달되지 않으며, 이동 에이전트 내부의 안전한 데이터 영역에 저장된다.

상거래 관련 정보는 협상정보, 결제정보, 배송정보 등과 같이 상품 구매에 필요한 정보로써 이동 에이전트로부터 Seller Host에게 전달된다. Seller Host는 이 정보를 바탕으로 구매 절차를 진행한다. 이러한 정보는 그림 7과 같이 Seller Host로부터 받은 RK로 암호화함으로서 보호된다. 그림 7은 암호화된 상거래 관련 정보를 보인다.

$$CD = E_{RK_{SH_x}}(CommercialData \mid H(CommercialData \mid SHID))$$

(그림 7) 암호화된 상거래 관련 정보

5. 결론

이동 에이전트는 전자상거래 환경에서 사용자의 요구 사항을 바탕으로 사용자가 원하는 상품을 검색, 협상, 구매의사 결정 등을 하는 자율적인 프로그램을 말한다. 이동 에이전트를 사용함으로써 나타나는 많은 장점에도 불구하고 이동 에이전트가 갖는 자체적인 보안 위험으로 인해 전자상거래 환경에 적용하는데 어려움이 있다. 특히 이동 에이전트가 가지고 있는 정보 및 데이터에 대한 위변조는 정확한 상품 구매를 방해하는 중요한 문제이다.

본 논문에서는 공개키 암호화 기법과 공유키 암호화 기법을 이용한 키 교환 메커니즘을 사용하여 이동 에이전트의 정보를 보호하는 기법을 제안했다. 본 기법은 호스트간의 이주를 통해 수집한 메타 데이터와 상품 구매에 필요한 정보를 Seller Host로부터 부여 받은 RK를 이용하여 암호화함으로서 데이터의 무결성을 보장한다.

이동 에이전트를 전자상거래 환경에 사용하기 위해서는 이동 에이전트의 정보 보호 외에도 이동 에이전트 코드 자체와 플랫폼에 대한 보안 연구가 이루어져야 한다. 보다 더 활발한 연구를 통해 이동 에이전트가 전자상거래 환경에서 중요한 요소로 활용되기를 기대한다.

참고 문헌

[1] A. Chavez and P. Maes, "Kahbah, An Agent Marketplace for Buying and Selling Goods," Proc. of the 1st Int'l Conf. on the Practical Application of Intelligent Agents and Multi Agent Tech., 1996.

[2] P. Dasgupta, L. E. Moser, and P. M. M. Smith, "MAgNET : Mobile Agents for Networked Electronic Trading," IEEE Trans. on Knowledge and Data Eng., vol. 11(4), pp. 509-525, 1999.

[3] A. Fuggetta, G. Picco, and G. Vigna, "Understanding code mobility," IEEE Trans. on Software Eng., vol. 24(5), pp. 352-361, 1998.

[4] A. Aneiba and J. S. Rees, "Mobile Agent Technology and Mobility," Proc. of the 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet 2004), 2004.

[5] C. G. Harrison, D. M. Chess, and A. Kershenbaum, "Mobile agents: Are they a good idea?," Technical report, IBM Research Report, IBM Research Division, T.J. Watson Research Center, Yorktown Heights, NY, 1995.

[6] S. Keegan and G. O'Hare, "EasiShop : Context Sensitive Shopping for the Mobile User through Mobile Agent Technology," Proc. of 13th Int'l. Symposium on Personal Indoor and Mobile Radio Communications (PAMRC 2002), 2002.

[7] G. Karjoth, D. Lange, and M. Oshima, "A Security Model for Aglets," IEEE Trans. on Internet Computing, vol(4), pp 68-77, 1997.

[8] N. M. Karnik and A. R. Tripathi, "A Security Architecture for Mobile Agents in Ajanta," Proc. of the 20th Int'l Conf. on Distributed Computing Systems, 2000.

[9] M. A. Mazlan, A. Samsudin, and R. Budiarto, "Secure Groups Communication for Mobile Agents Based on Public Key Infrastructure," Proc. of the 9th Asia-Pacific Conf. on Communications (APCC 2003), 2003.