유· 무선 통합 보안 e/m-Commerce 애플리케이션 설계 및 구현

김만수, 정목동
부경대학교 컴퓨터공학과
e-mail : kmansoo@mail1.pknu.ac.kr, mdchung@pknu.ac.kr

Development and Implementation of a secure e/m-Commerce Application which integrates wire and wireless environments

Mansoo Kim, Mokdong Chung
Department of Computer Engineering, Pukyong National University

요 약

정보통신기술의 발전으로 유· 무선 인터넷 사용자가 기하급수적으로 증가하고 있는 가운데 무선 인터넷을 이용한 m-Commerce 의 활성화가 기대되고 있다. 이와 더불어 무선 인터넷에서 안전한 m-Commerce 를 제공하기 위해서는 다양한 모바일 기기 환경에 맞춘 무선 인터넷 PKI 서비스가 요구된다. 본 논문에서는 모바일 기기 성능, 네트워크 환경, 서비스 종류, 사용자의 보안 요구 사항에 맞추어 경제학 이론에서 출발한 MAUT(Multi-Attribute Utility Theory)와 간결한 휴리스틱스(Simple Heuristics) 알고리즘을 이용한 보안 등급 프로토콜을 동적으로 결정하는 적응적 보안 정책 알고리즘을 제안한다. 이를 바탕으로 PKI 와 X9.59 기반의 보안 e/m-Commerce 를 구축한다.

1. 서론

정보통신기술의 발전으로 유· 무선 인터넷 사용자가 기하급수적으로 증가하고 있으며, 유선 인터넷 서비스와 무선 인터넷간 연동 서비스의 활성화가 기대되고 있다.

이렇듯 유· 무선 인터넷에 대한 수요가 증가하고 있는 가운데 무선 인터넷이 보다 활성화되기 위해서는 유선 인터넷 연동과 더불어 유선 인터넷의 응용서비스와 같은 증권거래, 계좌이체, 주문 등 전자상거래 서비스를 제공해야 하는데, 이러한 서비스가 성공적으로 활성화되기 위해서는 보안문제가 우선적으로 해결되어야 할 과제이다. 따라서 유· 무선 e/m-Commerce 에서 정보보호 및 상호인증 기술을 적용하기 위해서는 공개키 기반구조(PKI: Public-Key Infrastructure)[2,3]가 필수적이다.

또한 e-Commerce 에서 표준으로 채택되고 있는 XML 의 이동성은 데이터 무결성과 인증 메커니즘을 필요로 하는 B2B/B2C 거래에 이상적인 조건을 제공한다. 이런 필요성에 의해 IETF 와 W3C 의 XML-Signature Working Group 에서 "XML-Signature Syntax and Processing"[5,7] 명세서를 정의하였다. XML 전자 서명은 기존의 XML 기술들을 단순히 통합하는 것뿐만 아니라 다양한 애플리케이션의 도메인에 맞춰서 문서를 작성할 수 있게 해 주는 일관된 방법을 제공하고 있다.

최근에는 m-Commerce 를 위한 무선 인터넷 PKI 체계가 구축되고 있는 중이다. 이 체계는 기존의 유선 PKI 의 구성요소를 그대로 이용하며, 무선 환경에 적합하도록 기능을 최소한 변화시킨 것이다.

그러나 무선 인터넷 PKI 를 구축할 경우에는 유선과는 달리 클라이언트(무선 단말기)와 서버간의 제한된 대역폭, 클라이언트의 처리능력과 제한된 메모리를 고려해야 한다. 또한 기존 유선환경과는 달리 인증서 검증 메커니즘의 경량화가 필요하다[11,12,14].

현재의 e/m-commerce 프로토콜은 다양하고 안전한 교신 기법을 제공하지 못하고 있다. 이를 해결하기 위해서 본 논문에서 우리는 사용자들이 취급하는 정보나 거래 정보의 민감도에 의해 보안 등급을 동적으로 선택할 수 있는 알고리즘을 개발하고, 이를 적용한 프로토콜의 설계를 목표로 하고 있다.

또한 우리는 제안한 알고리즘과 프로토콜을 사용하여 모바일 환경에서 유선 인터넷과 같은 PKI 기반 정보보호 기술을 적용한 e/m-Commerce 보안 애플리케이

* 본 연구는 부경대학교 BK21 산업자동화 및 정보통신분야 인력양성사업단 지원으로 수행 되었음.

션을 설계 및 구현한다. 이 e/m-Commerce 보안 애플리케이션은 시스템환경, 네트워크 환경, 서비스요구사항 및 사용자 보안 정책 등 모바일 환경에 맞추어 보안/인증/지불 프로토콜을 적응적으로 선택한다.

논문의 구성은 1 절 서론에 이어서 2 절 관련 연구, 3 절 적응적 보안 정책 권고 알고리즘, 4 절 이카로스(Icarros) e/m-Commerce 구현, 5 절 결론과 향후 연구에 대해서 논한다.

2. 관련 연구

2.1. Public Key Infrastructure (PKI)

공개키 기반 구조(PKI)는 공개키 공개키 암호문을 처리하는 시스템이다. 공개키 암호문은 디지털 서명과 비대칭 암호학 모두 포함하고 있다. PKI 는 디지털 서명과 CA(Certification Authority)를 통해서 자동적으로 공캐키들을 관리하는데 사용된다. CA 는 최종 객체(end entity)를 인증하기 위해 디지털 인증서를 사용하는데, 이것은 주체(subject) 사용자가 합법적인 사용자임을 입증하기 위해 CA 의 개인키로 디지털 서명을 생성하고, 이것을 디지털 인증서에 첨부한다.

공개키 암호 알고리즘을 사용하는 정보 시스템은 안전성과 신뢰성을 제공하기 위해 주체 공개키에 대한 무결성과 인증성이 요구 된다. 공개키 기반구조는 기본적으로 암호 시스템 및 서명 시스템에서 요구되는 사용자 공개키에 대한 무결성과 인증성을 보장하기 위하여 인증기관에 의하여 발행되는 인증서에 바탕을 두고 있다

2.2. Account Authority Digital Signature (AADS)

AADS 모델은 ANSI X9.59 "Electronic Commerce for Financial Service Industry" 표준화 노력의 한 부분으로서 1997 년 Lynn 과 Anne Wheeler 에 의해 처음으로 소개 되었다[17, 18].

Wheeler, Lynn 과 ANSI X9A10 그룹은 AADS 아이디어를 구상했고, X9.59 표준에 이를 사용하였고, 몇몇 프로타입은 이미 개발되고 있다. Wheeler 과 Lynn 은 CA 기반의 인증서 시스템의 존재가 금융서비스 산업을 위한 비즈니스 모델에 필요성이 없다는 생각을 기초로 디지털 서명에 기반한 공개키의 검증을 위해 CA 의 인증서 증명에 대한 필요성을 없애려고 시도하였다.

이 모델에서의 공개키는 그 소유자의 계정기관(예를 들면 금융기관)에 저장되고 사용된다.

2.3. 관련 시스템

홍콩 대학에서는 모바일 e-Commerce 에서 End-to-end 의 보안을 위해 PKI 기반 응용 애플리케이션을 개발하였다[24]. 이 애플리케이션은 모바일 장비의 적은 메모리와 낮은 CPU 성능으로 인한 서비스 제공자의 X.509 인증서에 대한 검증의 어려움을 해결하기 위하여 ME(Mobile Equipment)와 MESS(SMS Gateway and Mobile Electronic Service Server)를 사용하였고, 통신은 Smart Card 를 이용한 SMS(Short Message Service)로 메시지를 암호화 하였다. 또한 모바일 기기의 인증을 대리하는 UAS(User Authentication Server)와 Server Provider 간의 인증을 위해서는 PESM(PKI End-to-end Secure Module) 모듈을 이용한 PKI 기반의 인증 프로토콜을 정의하였다. 그러나 이 애플리케이션에서 요구되는 Smart Card 는 아직 보편화되지 않았고, 이러한 Smart Card 를 제공하는 모바일 장비가 고가라는 점이 문제점이다.

미주리 대학에서는 e-Commerce 거래에서 참여자의 보안 레벨에 따라 보안 정도를 동적으로 변화 시키는 프로토콜과 이를 적용한 ASE-COM(Adaptive Secure e-Commerce) 시스템을 제안했다[19]. 이 시스템은 참여자의 보안 등급, 시스템의 성능, 네트워크의 상태 등을 휴리스틱 알고리즘을 사용하여 최적의 보안 프로토콜을 결정하는 시스템이다.

그러나 다양한 변수에 대한 선호도 결정 알고리즘은 단순한 휴리스틱스 알고리즘만 적용하는 것보다 휴리스틱스와 다중변수에 대한 정량적 의사 결정 방법인 MAUT 를 함께 적용하는 것이 보다 효율적일 수 있다.

3. 적응적 보안 정책 권고 알고리즘

불행하게도 현재의 e-Commerce 프로토콜은 다양한 보안 상호 작용 메커니즘을 지원하지 않는다. 이런 무제를 해결하기 위해 본 연구에서는 모바일 단말기의 종류, 서비스 형태, 참여자의 보안 선호도 및 정보의 중요성을 MAUT 와 간결한 휴리스틱스 알고리즘을 이용하여 보안 등급 프로토콜을 동적으로 결정하는 적응적 보안 정책 알고리즘을 개발한다.

이 알고리즘을 위하여 보안 등급을 위한 계수들을 정의한다.

(1): 시스템과 네트워크 성능에 대한 계수

comp	computational overhead for message encryption/decryption
sMsg	size of message
sKey	size of key
nType	type of network : LAN, WAN, Internet
tType	type of mobile terminals : old-fashioned or multimedia terminal

(2): 사용자의 보안 선호도 정도에 대한 계수

iSens	degree of information sensitivity
rCred	relying party's credit
pTime	peak time or not
cipher	cipher algorithm
resoc	available resource such as time, cost, etc

다음은 보안 등급을 결정하는 알고리즘이다.

```
function SecuLevel(secureProblem) returns sLevel
inputs: secureProblem    : Determining security level
static:
 // Utilization of domain independent knowledge such as
 // system and network capabilities
step 1
      SysNet(); // calculate sLevel  by applying domain
                // independent variables such as comp, sMsg,
                // sKey, nType, and tType
```

```
// Utilization of domain dependent knowledge such as
// MAUT and Simple Heuristics
step 2 // Determining security level by applying domain
       // dependent variables
   MAUT(); // A utility function can be determined by the
           // interaction with the user according to MAUT
           // using domain dependent variables (iSens,
           // rCred, pTime, cipher, resoc)
   Update(); // adjust sLevel  according to the value of
           // u(x1,x2,..,xn)
   TakeTheBest() // If users don't want to use MAUT, we can
adjust sLevel using Simple Heuristics
End SecuLevel;
```

```
// A utility function can be determined by the interaction with
// the user according to MAUT using domain dependent
// variables (iSens, rCred, pTime, cipher, resoc)
function MAUT() returns a utility function
static u(x1, x2, ...xn) : a utility function
u(x1, x2, ...xn) = k1u1(x1) + k2u2(x2) + ... + knun(xn);
// where ui(x°i) = 0, ui(x*i) = 1, and ki is constant for all i.
// ui(xi ) is determined as follows by the interaction with the
user
if risk prone then b(2^cx -1);
else if risk neutral then bx;
     else if risk averse then blog2(x+1);
// where b, c > 0 constants
return u(x1, x2, ...xn);
nd MAUT;
```

4. 보안 e/m-Commerce 애플리케이션 – 이카로스

3 절에서 제안한 적응적 보안 정책 권고 알고리즘을 적용한 e/m-Commerce 보안 애플리케이션인 이카로스(Icarus)는 무선 인터넷 환경에서 모바일 기기의 성능, 네트워크 환경, 서비스 정책 및 사용자 보안 등급을 MAUT 와 간결한 휴리스틱스를 이용하여 적응성 있게 보안/결제/인증 프로토콜을 결정하는 시스템이다.

그림 1 은 Icarus 의 시스템 구성도이다.

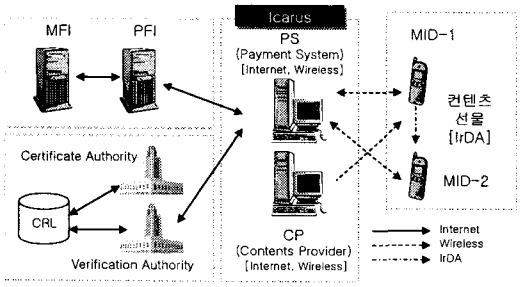

그림. 1 System Overview of Icarus

그림 1 에서 보여지는 것처럼 모바일 기기(MID:Mobile Information Device)는 m-Commerce 서비스를 위해 우선 보안 등급 프로토콜을 결정한다. 이 프로토콜 결정에 의해 MID 는 PS 에게 데이터가 전송이 되면, PS 는 PKI 또는 X9.59 기반 보안 프로토콜인지 여부를 수신된 데이터를 통해 확인한다. PS 에 의해 확인된 보안 프로토콜은 MID 의 서비스가 종료될 때까지 유지된다. 시스템의 각 요소들은 프로토콜 내부에 적용된 암호 알고리즘과 키에 대해서 분석하고 이를 보안/인증/결제 서비스에 사용한다.

그림 2 는 X.509 인증서를 기반으로 인증서의 생성, 쇼핑, 결제과정을 보여준다. 이 과정은 모바일 기기의 높은 성능, 빠른 데이터통신 등의 모바일 환경에서 적용되는 프로토콜이다. 이것은 유선 인터넷의 X.509 기반과 동등한 보안 성을 보장한다.

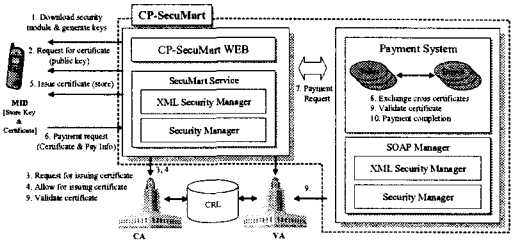

그림. 2 X.509 base Payment Progress

또한 이카로스는 모바일 기기의 성능과 네트워크 환경이 X.509 인증서 기반 보안을 만족시킬 수 없을 경우 X9.59 프로토콜, 보안 알고리즘 변경 및 키 크기 변경 등의 적응적 보안 결정 알고리즘에 의해 보안 프로토콜을 선택한다.

그림 3 은 X9.59 기반의 AADS 프로토콜에 대한 XML 결제 스키마를 보여준다.

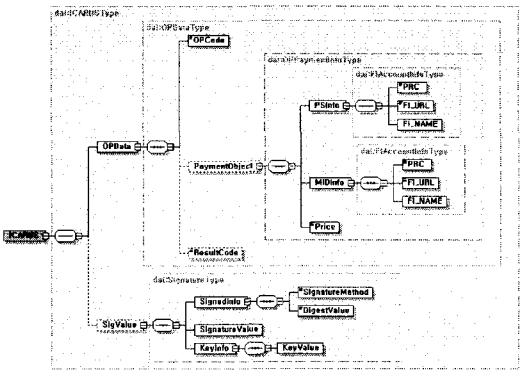

그림. 3 XML Schema for X9.59 Payment Protocol

AADS 프로토콜은 CA 를 사용하지 않고, MID 와 PS 가 그들의 금융 기관에 의해 상대방의 공개키를 인증하는 것이다.

그림 4 는 ① PS 의 공개키를 PS 의 계정 기관인 PFI(PS's FI)가 서명을 하여 MFI 로 보내면, ② MFI(MID's FI)는 이를 PFI 의 공개키로 서명확인 후 자신의 개인키로 PS 의 공개키에 대해서 서명한다. ③ MID 는 이것을 MFI 의 공개키로 서명을 검증하여 PS 의 공개키을 인증하는 과정이다.

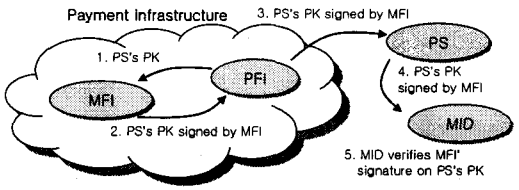

그림. 4 MID's PS's Public Key Authentication Progress

5. 결론

유선 인터넷 서비스와 무선 인터넷간 연동 서비스가 활성화되면서 유선 인터넷 PKI 기반 정보보호 기술과 같은 보안성이 무선 인터넷에서도 요구되고 있다. 그러나 다양한 모바일 환경이 공존하는 무선 인터넷에서의 보안적용에 많은 어려움이 있다.

따라서 본 논문에서는 무선 인터넷의 단말기의 성능, 네트워크 환경, 서비스요구사항 및 사용자 보안정책 등 여러 가지 상황을 고려하여 MAUT 와 간결한 휴리스틱스 알고리즘을 이용하여 보안/인증/결제 프로토콜을 동적으로 결정하는 알고리즘을 제안하였고, 이를 적용한 적응성 있는 유. 무선 통합 e/m-Commerce 보안 애플리케이션인 이카로스를 설계 및 구현하였다. 이카로스는 무선 인터넷 환경에서 적응성 있는 프로토콜 결정에 의해 결제 시스템, 암호 알고리즘, 키 크기 등을 고려한 보안 등급을 조정함으로써 m-Commerce 에서 안전한 보안/인증/결제 과정을 수행 할 수 있었다.

본 논문에서 설계 및 구현한 e/m-Commerce 보안 애플리케이션은 Java 와 XML 기반으로 설계되고, 다양한 보안 알고리즘을 사용하여 플랫폼 독립성을 유지하면서 모바일기기에서 안전한 거래와 결제를 보장한다.

참고문헌

[1] http://www.kisa.or.kr, "Wireless PKI," 2001.5.
[2] RSA, S., "Understanding Public Key Infrastructure (PKI)," 1999, RSA Security Inc.
[3] Berkovits Shimshon et al., "Public Key Infrastructure Study: Final Report," *Produced by the MITRE Corporation for NIST*, April 1994.
[3] RFC: 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 1996.
[4] W3C, Extensible Markup Language (XML), http://www.w3c.org/XML, February 1998.
[5] www.w3.org "XML Signature Requirements WD," W3C Working Draft, October 14, 1999.
[6] http://www.w3c.org, "XML-Signature Syntax and Processing" W3C Recommendation, February 12, 2002.
[7] http://www.w3c.org, "XML Encryption Syntax and Processing," W3C Working Draft, October 18, 2001.
[8] http://www.w3c.org, "Decryption Transform for XML Signature," W3C Working Draft, October 18, 2001.
[9] Gunther Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems," *Proceedings of Esorics98, LNCS 1485*, Springer-Verlag, 1998, pp277-293.
[10] P.Gutterman, "PKI: It's Not Dead, Just Resting," IEEE Computer, Vol. 35, No. 8, 2002, pp. 41-49.
[11] M.Soriano and D. Ponce, "A security and usability proposal for mobile electronic commerce," *IEEE Communications Magazine*, Vol. 40 Issue: 8, Aug. 2002, pp. 62 -67.
[12] Tang Jian and J. Veijalainen, "Using agents to improve security and convenience in mobile E-commerce," *Proceedings of the 34th Annual Hawaii International Conference on*, 2001, pp. 3540 -3549.
[13] S.S.Y.Shim et al., "Business-to-business e-commerce frameworks," *IEEE Computer*, Vol. 33 Issue: 10, Oct. 2000, pp. 40 -47.
[14] N. EI-Fishway et al., "An effective approach for authentication of mobile users," *Proceedings of Vehicular Technology Conference*, 2002. VTC Spring 2002. IEEE 55th, Vol. 2, 2002, pp. 598-601.
[15] R.L.Keeney and H.Raiffa, "Decisions with Multiple Objectives: Preferences and Value Tradeoffs", John Wiley & Sons, New York, NY, 1976.
[16] G.Gigerenzer et al., "Simple Heuristics That Make Us Smart", Oxford University Press, New York, 1999.
[17] A.Wheeler, and L.Wheeler, "Payment, Security & Internet References," http://www.garlic.com/~lynn.
[18] Albert Levi, Cetin K. Koc, "CONSEPP: Convenient and Secure Electronic Payment Protocol based on X9.59," *Proceedings of 17th Annual Computer Security Applications Conference*, 2001, New Orleans, Louisiana.
[19] Sung Woo Tak et al., "Design and evaluation of adaptive secure protocol for E-commerce," *Proceedings of Tenth International Conference on Computer Communications and Networks*, 2001, pp 32 -39.
[20] W.Diffie and M.Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, vol.22, no. 6, 1976, pp.644-654.
[21] "Information Technology? Open Systems Interconnection? The Directory Authentication Framework," ISO/IEC 9594-8, 1993, also ITU-T Recommendation X.509, v2.
[22] C. Ellison, "SPKI Requirements," RFC 2692, Sept, 1999, http://www.ietf.org/rfc2692.txt.
[23] P.Hope, "Certificate Revocation: Why You Should Do It and Why You Don't," login, Dec, 2001,pp.36-40, http://www.usenix.org/publications/login/index.html.
[24] Tin-Wo Cheung; Chanson, S.T, "Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-Commerce," In the *Proceedings of the Second International Conference on Web Information Systems Engineering 2001*, Volume: 1, 2001, pp. 3 –7.