제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

PKI 기반 e-Commerce 보안 애플리케이션 설계

김만수, 김환조, 정목동
부경대학교 컴퓨터 공학과
e-mail : {kmansoo, xxrcn}@mail1.pknu.ac.kr, mdchung@pknu.ac.kr

Design of PKI based e-Commerce Security Application

Mansoo Kim, Hwanjo Kim, Mokdong Chung
Dept. of Computer Engineering, Pukyong National University

요 약

초고속 통신망을 이용한 인터넷의 대중화와 더불어 인터넷을 기반으로 하는 e-Commerce 가 활발해지고 있다. e-Commerce 에 있어서 민감한 정보의 기밀성과 사용자 인증의 확보가 필수적이며, 이를 위해서는 전자 서명 기술을 포함하고 있는 공개키 기반의 인증서 관리 체계의 확립이 선결되어야 한다. 본 논문에서는 인증, 기밀성 및 무결성 문제를 해결하기 위해 PKI 기반 인증서의 생성, 관리 기능과 인증서를 상호 교환하여 매매 협상을 하는 에이전트 중재에 의한 SecuPmart 보안 애플리케이션을 설계하고 이에 대하여 기술한다.

1. 서론

인터넷의 급성장에 따라 e-Commerce 시장의 규모 또한 급격히 증가하고 있다. 하지만 e-Commerce 의 성공을 위협하는 요소도 여러 가지 있는데 그 중 가장 큰 것은 보안에 관한 것일 것이다. e-Commerce 시스템은 공개키 암호 시스템에 바탕을 두고 실현되어야 사용자 공캐키의 신뢰성과 안전성을 보장 받을 수 있다.

공개키 기반 구조(PKI: Public Key Infrastructure)[1]는 공개키 암호 방식을 사용하는 암호 시스템에서 사용자의 공개키를 안전하고 신뢰성 있게 공표하는 수단을 제공한다. 따라서 안전하고 신뢰성 있게 사용자의 공개키를 공표하기 위한 공개키 기반 구조는 인터넷 e-Commerce 시스템에서 매우 중요한 역할을 수행할 것이다.

이와 더불어 XML 기술이 인터넷 e-비즈니스 시스템 등에서 메시지 교환 형식으로 이용되면서 이들 XML 문서의 보안 역시 필수적 요구 조건이 되고 있고, 안전한 e-Commerce 를 수행하기 위해서 XML 디지털 서명(Digital Signature)은 반드시 지원 되어야 한다[2][3][4][5][6].

따라서 본 논문에서는 e-Commerce 에서 표준으로 자리 잡고 있는 PKI 기반의 X.509 인증서를 이용한 안전하고 신뢰할 수 있는 e-Commerce 보안 애플리케이션을 설계하는데, 상호 인증을 위해 PKI 기반 보안 애플리케이션 SecuPmart 를 설계하고, 또 매매 에이전트의 협상 정보의 보안과 매매에 대한 부인 방지 문제를 해결하기 위해 PKI 와 XML 기반 전자 서명 프로토콜을 설계한다.

본 논문에서 설계한 e-Commerce 애플리케이션은 Java 와 XML 기반으로 설계되고 인증서의 검증 및 기밀 정보의 암,복호화가 클라이언트 측 보안 모듈에서 처리되므로 현재 웹 보안의 문제점을 플랫폼 독립적으로 해결할 수 있다.

논문의 구성은 1 절 서론에 이어서 2 절 관련 연구, 3 절 XML 과 PKI 기반 보안 애플리케이션 SecuPmart 시스템 설계, 4 절 결론과 향후 연구에 대해서 논한다.

2. 관련 연구

2.1 공개키 기반 구조(PKI: Public Key Infrastructure)

공개키 암호 시스템은 비대칭 키 암호 시스템이라고도 불리며, 수학적 함수를 기반으로 하여 비밀키 암호 시스템과 달리 키 쌍이 존재하여 하나의 키는 누구든지 사용할 수 있도록 공개하며 다른 하나는 자신만이 비밀스럽게 보관하는 방식을 말한다. 이때 공개하는 키를 공개키(public key)라고 하며 비밀스럽게 보관하는 키를 개인키(private key)라고 한다.

공개키 기반 구조는 공개키 인증서에 바탕을 두고 구축되어야 한다. e-Commerce 를 위한 대부분의 보안

응용은 공개키 알고리즘에 바탕을 두고 있다.

인증서는 CA(Certification Authority)가 최종 객체(end entity)를 인증하는 전자 증명서 역할을 수행하며, 주체(subject) 사용자가 합법적인 사용자임을 입증하기 위해 CA 는 자신의 개인키로 디지털 서명문을 생성하여 인증서에 첨부한다. 인증서에는 인증서 사용자에 대한 공개키와 신분에 대한 정보들을 포함하고 있다.

2.2 XML 전자 서명(XML Digital Signature)

최근 XML[2]은 B2B 와 B2C 등과 같은 기본적인 응용과 더불어 여러 분야에 적용할 수 있는 기술로 각광 받고 있다. 한편 e-Commerce 상에서의 대부분의 서비스가 전자적으로 처리됨에 따라 그에 따른 보안의 중요성이 대두되고 있다. 특히, XML 을 활용한 e-Commerce 상의 문서 교환 과정의 보안에 대한 표준화 작업이 활발히 진행되고 있는데, XML 전자 서명은 IETF 와 W3C 의 XML-Signature Working Group 에서 제정된 "XML-Signature Syntax and Processing" 명세서[4]에서 XML 디지털 서명의 구문과 처리 과정을 기술하고 있다.

XML 전자 서명을 사용하기 위한 보안 관련 고려사항은 다음과 같다.

(1) 기밀성(Confidentiality): 전송되는 자료의 일부 또는 전부를 제 3 자가 볼 수 없도록 하는 기능.
(2) 인증(Authentication): 사용자 인증은 사용자가 정당한 사용자임을 증명하는 기능.
(3) 무결성(Integrity): 원격지에서 전송된 문서가 위, 변조되지 않았음을 증명하는 기능.
(4) 승인(Authorization): 거래 요청에 대하여 상대방의 거래를 인증하고 이에 대한 처리 결과를 거래 요청자에게 통보하는 기능.
(5) 부인방지(Non-Repudiation): 문서를 송, 수신하는 경우 해당자가 송, 수신에 대한 행위를 부인할 수 없도록 하는 기능

2.3 Pmart 및 관련 시스템

Pmart[9][10]는 본 연구실에서 개발한 다중 변수 기반 에이전트 중재 e-Commerce 시스템이다. Pmart 에서 매매는 판매 및 구매의 협상 정보를 가진 에이전트간에 이루어진다. Pmart 의 협상 모델은 영역 지식과 일반 지식을 동시에 사용할 수 있는데, 영역 지식은 MAUT (Multi-Attribute Utility Theory) [7]에 바탕을 두고 있고 일반 지식은 기존의 구매 기록(purchase history)과 간결한 휴리스틱스(simple heuristics) [8]에 바탕을 두고 있다.

홍콩 대학에서는 모바일 e-Commerce 에서 End-to-end 의 보안을 위해 PKI 기반 응용 애플리케이션을 개발하였다[11]. 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[13]. 이 시스템은 참여자의 보안 등급, 시스템의 성능, 네트워크의 상태 등을 휴리스틱 알고리즘을 사용하여 최적의 보안 프로토콜을 결정하는 시스템이다.

3. XML 과 PKI 기반 보안 애플리케이션 - SecuPmart

3.1 시스템 구성

SecuPmart 는 자체적인 CA 를 운영한다. 각 SecuPmart 는 CA 로부터 인증서를 발급 받고, 고객 컴퓨터에 다운로드 된 보안 모듈에서 SecuPmart 의 인증서를 검증한다. 검증된 인증서의 공개키는 e-Commerce 에서 안전한 거래를 위해 협상 정보, 결재 정보 등의 암호화에 사용된다.

그림 1 은 SecuPmart 시스템 구성을 보여준다. 판매자와 구매자는 웹 브라우저를 사용하여 SecuPmart 에 접속한다. SecuPmart 와 Pmart 에이전트 시스템은 각각 분리된 시스템일 수도 있고, 하나의 시스템으로 구성될 수도 있지만, SecuPmart 와 Pmart 에이전트 시스템은 반드시 방화벽이 있는 로컬 네트워크 안에 위치되어야 한다.

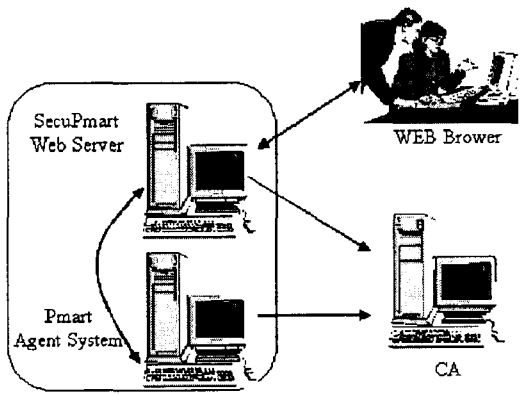

그림 1. SecuPmart 전체 시스템 구성도

그림 2 는 고객-SecuPmart-CA 간 X.509 인증서 사용으로 안전한 매매 과정을 보여준다.

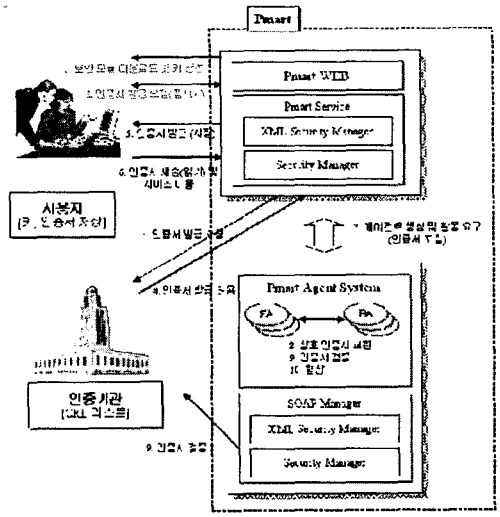

그림 2. SecuPmart 보안 절차

각 단계별 설명은 다음과 같다.

1. 고객은 SecuPmart 에서 상품의 매매를 위해 인증서를 발급 받아야 한다. 처음 인증서 생성 과정에서 SecuPmart 의 보안 모듈을 다운 받는다. 보안 모듈은 Java Web Start 기술로 실행되며 PKI 기반 암호화를 위해 공개키와 비밀키를 생성하여 고객 컴퓨터의 하드 디스크나 플로피에 저장하고, 이를 관리한다.
2. 고객은 SecuPmart 에 인증서 생성에 필요한 정보와 공개키를 SecuPmart 의 공개키로 암호화 하여 보낸다.
3. Pmart 시스템은 CA 에 사용자 인증을 위한 인증서를 발급 요청한다..
4. CA 는 Pmart 로부터 요청된 인증서 발급을 허가하여 인증서를 보낸다.
5. 보안 모듈은 발급된 인증서를 하드 디스크에 저장한다.
6. 고객은 상품을 검색한 후 구매 에이전트 생성을 위해 구매 정보와 함께 발급된 인증서를 SecuPmart 로 전송한다.
7. 물품 구매를 위한 에이전트를 생성한다.
8. 구매 에이전트는 판매 에이전트를 찾아 상호 인증서를 교환한다.
9. 인증서를 CA 로부터 검증 받는다.
10. 인증이 된 후에 상호 협상을 진행한다. 협상을 위해서는 먼저 세션키를 생성하고, 협상 정보를 암호화한다.

3.2 시스템 계수

표 1 은 본 논문에서 인증서의 생성 및 안전한 매매에 필요한 시스템의 계수에 대한 설명이다.

표 1. 시스템 계수

계수	설명
CA	인증 기관
PM	SecuPmart
C_x	고객 x
PU_{C_x}	C_x의 Public Key
PR_{C_x}	C_x의 Private Key
$E_y(m)$	키 y를 사용해 메시지 m을 암호화
$D_y(m)$	키 y를 사용해 메시지 m을 복호화
$Info_{C_x}$	인증서 생성을 위한 C_x의 정보
$Cert_{C_x}$	C_x의 인증서
$CRL_y(Cert_{C_x})$	$Cert_{C_x}$를 개인키 y 를 사용하여 폐기 되었음을 확인
$V(Cert_{C_x})$	$Cert_{C_x}$를 검증

3.3 인증서 생성 절차

고객이 e-Commerce 상에서 자신을 증명하기 위해서는 인증된 CA 가 서명한 인증서를 발급 받아야 한다. 그림 3 은 인증서 발급을 위한 각 단계를 보여준다.

다운로드 된 보안 모듈은 공개키와 비밀키를 생성하고 인증서 생성에 필요한 정보와 공개키를 SecuPmart 의 공개키로 암호화 하여 보낸다. SecuPmart 에서는 자신의 비밀키로 복호화 하고, 다시 CA 의 공개키로 암호화 하여 전송한다. CA 는 X.509 공개키를 생성하고, 자신의 비밀키로 전자 서명을 하여 합법적인 사용자임을 보장한다.

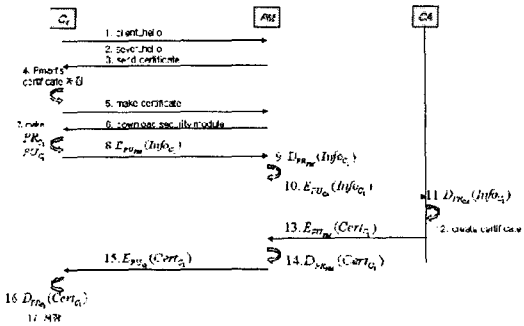

그림 3. 인증서 생성 과정

인증서 생성 정보와 발급된 인증서는 XML 문서로 교환되며, 중요 정보는 XML 엘리먼트(Element) 단위로 암호화를 한다. 인증서 생성 정보에 대한 XML DTD 는 다음과 같다.

```
<!ELEMENT validity_period (notbefore, notafter)>

<!ELEMENT DAICertificateCreateInfo
  (X500Name, validity)>
```

```
<!ELEMENT X500Name
  (c_name, o_unit, organization, local, county)>

<!ELEMENT validity (validity_period)>

<!ELEMENT DAICertificate
  (version?, issuer, subject, delegation?, tag, validity,
 comment?), cert>

<!ELEMENT issuer (X500Name)>
<!ELEMENT subject (X500Name)>
<!ELEMENT cert (#PCDATA)>
```

3.3 상호 검증 절차

SecuPmart 에서 고객은 상품을 구매하기 위해 구매 에이전트를 생성해야 한다. 구매 에이전트는 판매 에이전트와 협상을 하여 상품에 대한 최적의 조건으로 구매를 진행한다. 구매 에이전트 생성을 위해 고객은 상품에 대한 구매 정보를 다중 변수 기반에 준하여 입력한다. 이러한 정보는 XML 로 표현되고, 이 XML 에서는 전자 서명이 첨부된다. 그림 4 는 두 에이전트의 상호 인증 과정을 보여준다. 구매 정보와 함께 자신의 인증서를 SecuPmart 에 보낸다. Pmart 는 고객의 구매 정보에 맞는 구매 에이전트를 생성하고, 에이전트 시스템에 등록시킨다.

협상의 시작은 먼저 구매 에이전트가 판매 에이전트에게 협상 요청과 함께 구매 에이전트의 인증서를 보낸다. 판매 에이전트는 CA 로부터 인증서를 검증하고, 인증서가 타당하면 판매 에이전트의 인증서를 보내 협상을 수락한다. 구매 에이전트는 역시 판매 에이전트의 인증서를 검증하고, 입찰을 요구한다.

입찰 정보는 구매 에이전트와 판매 에이전트 간 세션키를 생성하고, 상호간 보안 데이터 전송을 한다.

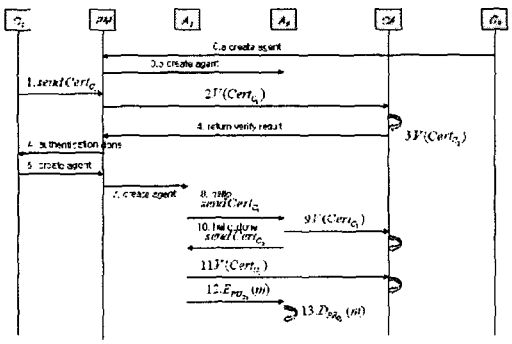

그림 4. 상호 인증과 협상 과정

4. 결론

본 논문에서는 e-Commerce 상에서 안전한 거래를 보장하고 부인 방지를 위해 PKI 기반 보안 애플리케이션인 SecuPmart 와, XML 기반의 프로토콜을 설계하였다. SecuPmart 는 고객이 자신을 증명하기 위한 인증서를 CA 로부터 발급 받고, 이를 검증하고, 관리하는 과정을 보여주었고, SecuPmart 의 모든 문서 교환 정보는 XML 로 표현하였고, XML 문서 내 기밀 정보가 담긴 엘리먼트들만 암호화하고, 문서 전체에 디지털 서명 함으로써 거래의 안정성 및 부인 방지를 보장하였다.

또한 본 논문에서는 SecuPmart 애플리케이션을 제시함으로써 e-Commerce 보안에 관련된 여러 문제들을 플랫폼 독립적으로 해결할 수 있는 하나의 방법을 제시하였다.

향후 인증서의 폐기에 따른 CRL(Certificate Revocation List)의 배포와 CA 의 키 갱신에 따른 기존 인증서의 인증 방법에 대한 연구가 필요하다.

참고 문헌

[1] RFC: 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 1996.

[2] W3C, Extensible Markup Language (XML), http://www.w3c.org/XML, February 1998.

[3] www.w3.org "XML Signature Requirements WD," W3C Working Draft, October 14, 1999.

[4] www.w3c.org "XML-Signature Syntax and Processing" W3C Recommendation, February 12, 2002.

[5] www.w3c.org "XML Encryption Syntax and Processing," W3C Working Draft, October 18, 2001.

[6] www.w3c.org "Decryption Transform for XML Signature," W3C Working Draft, October 18, 2001.

[7] R.L.Keeney and H.Raiffa, Decisions with Multiple Objectives: Preferences and Value Tradeoffs, John Wiley & Sons, New York, NY, 1976.

[8] G.Gigerenzer et al., Simple Hueristics That Make Us Smart, Oxford University Press, New York, 1999.

[9] Mokdong Chung and Vasant Honavar, "A Negotiation Model in Agent-mediated Electronic Commerce," *Proceedings of the IEEE International Symposium on Multimedia Software Engineering*, Taipei, Dec. 2000, pp. 403-410.

[10] 정목동, "다중변수 기반 에이전트 중재 전자상거래 협상 모델 및 프레임워크 설계," *정보과학회논문지 : 소프트웨어 및 응용*, 28 권, 11 호, 2001, pp.842-854.

[11] Tin-Wo Cheung; Chanson, S.T, "Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce," *Proceedings of the Second International Conference on Web Information Systems Engineering 2001, Volume: 1* , 2001, pp. 3 -7

[12] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," *Advances in Cryptology -- Crypto'97*, Springer-Verlag, 1997.

[13] 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