XML 전자서명을 이용한 다중인증 멀티 에이전트시스템*

김 귀 남**

요 약

정보화 시대의 요구에 대한 교육적 대응은 학습자중심의 교육이며, 정보통신 기술을 기반으로 한 원격 교육이다. WBI(Web Based Instruction)는 웹을 매체로 활용하여 원거리에 있는 학습자를 교육시키는 형태로서 교수자와 학습자간 상호작용을 가능하게 하고, 다양한 형태의 학습 자료를 제공하며, 공간적 제약을 극복할 수 있다는 장점이 있다. 차세대 웹 표준문서 포맷으로 부상되고 있는 XML(eXtensible Markup Language)을 사용한 규격에 대한 국내외적인 표준화 작업이 가속화되고 있으며, 최근 XML 보안에 대한 연구가 활성화 되고 있다. XML 보안은 XML 엘리먼트 암호화, XML 전자서명, XML 접근제어 등으로 분류되는데 특히 XML 전자서명은 XML문서를 이용하는 여러 분야에 사용되어 전자서명 시스템간의 상호 연동성을 높일 수 있다. 본 논문에서는 웹상에서 사용되어지는 공인인증서에 대한 사용자의 ID, PW로 인한 보안적 측면을 고려한 방법으로 XML 전자서명 기법을 이용한 다중인식 원격교육 에이전트 시스템을 제안 하였다.

Multi-Certification of Agent System Using XML*

Kuinam J. Kim**

ABSTRACT

Internet becomes absolutely necessary tools due to rapid progress of information technology. Educational correspondence about an age of information demand is focused on a learner and remote education based on information technology. WBI(Web Based Instruction) is a formation that remotly educate a learner using web, possible mutual reaction between instructor and learner, submit various studying material, has a good point to overcome spatial restriction. Internal and external standardization working is accelerated and recently XML security studies are activated using XML which is next generation web standard document format. In this paper, we propose multi-Certification of agent system using XML digital signature to satisfy security requirement.

Key words : Multi-Certification, XML, WBI, Digital Signature

* 본 연구는 2004년 경기대학교 교내연구비 지원으로 수행되었음.

** 경기대학교 정보보호기술공학 교수

1. 서 론

WWW(World Wide Web)의 등장이후, 원격교육은 이제 선택이 아니라 필수적인 요소가 되었다.

현재 뿐만이 아니라, 미래의 교육은 단일 시스템상의 컴퓨터를 이용한 학습방식에서 네트워크를 통한 학습으로 전환되리라는 것은 당연한 명제이다. 이러한 변화는 PC통신 및 네트워크의 대중화에 따라 인터넷의 사용이 보편화됨에 따라, 자연스럽게 발생한 현상이라 할 수 있다.

원격교육은 Distance education, Tele-education, Open-education 표현되며, 먼거리에 있는 학습자들에게 다양한 매체와 기술을 사용한 계획된 교수·학습경험으로 학습자 상호작용을 격려하고 학습을 인증하는 것이다[6]. 이러한 WBI (Web Based Instruction)는 웹을 매체로 활용하여 원거리에 있는 학습자를 교육시키는 형태로서 교수자와 학습자간 상호작용을 가능하게 하고, 다양한 형태의 학습 자료를 제공하며, 공간적 제약을 극복할 수 있다는 장점이 있다[7]. 원격교육을 원활히 하기 위하여 보안은 필수 요소인데 현재 사용하는 보안기법으로는 공인인증서와 전자서명이 그 대표적이라 할 수 있다.

전자서명이란 상대방에게 송신자의 신뢰성을 증명해주는 방법이로, 임의의 공격으로 인한 문서 위조를 방지하기 위한 기법으로, 상대방에게 전자적으로 작성된 서명이 첨부된 형태의 문서를 전송하여 수진자로 하여금 확인 가능하게 하는 것이다.

그러나 매번 사용할 때 마다 무료로 발급되던 전자 금융거래 공인인증서가 2004년 6월부터 건당 약 4400원을 지불해야 하는 유료 서비스로 전환된다. 또 공인인증서는 1년마다 다시 발급받도록 되어 있고, 만약 분실 시에도 다시 받아야 되므로, 고객의 대한 부담은 더더욱 늘어갈 수밖에 없다.

이러한 문제점을 해결하기 위하여 본 논문에서는 WBI에서의 보다 효과적이고 실용적인 보안을 위한 다중인증 기법을 제안하고자 한다.

2. 관련 연구

2.1 인증서 관련 분석

인터넷뱅킹, 증권거래시스템, 전자입찰 등과 같은 온라인 서비스의 경우, 사용자의 보호를 위해 인증서를 이용한 보안을 하고 있다. 그러나 기존의 원격교육 시스템에서는 패스워드 방식의 온라인 서비스를 하고 있기 때문에 보안적인 측면에서는 전혀 무방비 상태라 할 수 있다.

인증서 기반의 온라인 서비스는 다음과 같은 기능을 가진다. 첫째, 대면에 의한 신원확인을 받기 때문에 신뢰성이 보장된다. 둘째, 서비스 정보에 대한 저자서명으로 사용자와 서비스 제공자간의 통신구간에서 변조되지 않았다는 무결성이 검증된다. 셋째, 서비스 제공자는 사용자의 전자서명 데이터를 보관하여 부인방지가 가능하다[2].

이러한 기능을 보장받기 위해서는 사용자는 본인의 개인키를 관리해야 하는 의무가 있다. 그러나 개인키 분실, 자격상실, 키 변경 등의 이유로 인증서의 폐지가 가능하다. 이런 경우 검증자는 수신한 인증서 상태가 유효한 것인지를 확인해야 한다[3]. 이를 위해 인증서 폐지목록인 CRL[4]과 실시간 인증서 상태를 제공하는 OCSP가 제안되었다[5].

고부가가치의 온라인 서비스는 실시간의 인증서 상태가 제공되지 않는다면 거래 쌍방의 분쟁 가능성이 존재한다. 이러한 이유로 CRL은 고부가가치의 온라인 서비스에 적합하지 않다[8].

문서 전송이 있을 때마다 CA를 통하여 인증서를 받아야 하는데 매번 받을 때마다 수수료를

내야 한다는 문제점이 발생한다. 또한 CA는 RA를 거쳐 CRL까지 걸쳐지는 시간적 문제와 여러 단계를 걸쳐지는 번거로움이 발생한다. 특히 고액의 주식 거래나 전자상거래에서 실시간 인증서 상태 검증은 반드시 필요하다. 실제 원격교육 시스템에서도 매번 이와 같은 일을 반복하게 되면 CA 및 RA에 있는 서버까지 과부하가 걸리게 되어 신뢰도가 떨어지게 된다. 현재 사용되는 인증서폐지목록 방법은 CRL과 Delta CRL을 사용하고 있는데 "이종의 시스템에서 OCRS를 이용한 효율적인 인증서 상태 검증에 의하면 CRL 및 Delta CRL의 단점을 다음과 같이 지적하고 있다[9].

2.1.1 CRL 단점

주기적인 인증서 발행으로 인해 실시간 인증서 상태를 제공해 주지 못하며, 사용자는 CRL을 매번 다운로드 받아야 하기 때문에 네트워크 비용이 많이 든다는 문제점이 있다.

2.1.2 Delta CRL의 단점

Delta CRL은 CRL의 단점을 개선하고자 가장 최근에 폐지된 인증서만을 포함하는 인증서 폐지 목록이다. 하지만 이역시도 완벽한 실시간성을 제공해 줄 수 없다는 문제점이 있다.

위에서 살펴 본 바와 같이 실시간이 떨어지게 되면 서버로부터의 응답시간이 느려지게 되어 위급한 입찰 및 수시로 변하는 입찰변화에 대한 Query 역시 늦어지게 된다. 이를 보완하고자 OCSP가 제안되었다.

OCSP를 단점을 살펴보면 다음과 같다. OCSP는 기존의 CRL 방식이 실시간 인증서 상태 정보를 제공해 주지 못한다는 문제점을 해결하기 위해 제안되었다. 하지만, 각각의 인증서에 대해 실시간적으로 인증서 폐지 여부를 확인하고 전자 서명해야 하므로 OCSP 서버는 과부하가 걸리게 된다는 문제점을 가지고 있어 상용화 단계에는 적용시키지 못하고 있는 실정이다.

따라서 기존 인증서 서명의 공인인증서 검증 방법인 CRL, Delta CRL, OCSP방법은 CA산하에 있는 각종 금융은행 및 증권사를 묶고 있는 CA 및 RA에 인증서 유효상태를 매번 검색해야 하는 문제점을 가지고 있다.

2.2 원격교육 시스템

현재 웹상의 모든 원격교육 시스템을 보면 보안측면에서 너무나 허술한 측면이 많다. 현재까지는 공인인증서를 꼭 사용해야 한다는 의무화되어 있지 않으며, 우리나라 현실에서 대대분의 원격교육 시스템을 사용하고 있는 사람은 학생들이어서 금전적인 문제로 아직까지 원격교육 시스템에서 공인인증이 사용되지 않고 있는 실정이다. 또한 관리자들의 보안 의식도 많이 부족한 상태이다. 다행히 정부에서 공인인증서를 권장하고 앞으로 웹상에서의 모든 결제는 공인인증을 하도록 발전해 나가려 하고 있다.

현재 웹상의 원격교육 시스템에서 문제점은 다음과 같다.

첫째, 우선 사용자들의 개인정보 보호가 잘 이루어지지 못하다는 점이다. 한국정보보호진흥원에서 최근 실시한 조사 결과 20%정도의 이용자들이 주민번호를 도용당한 경험이 있으며, 또 타인의 주민번호를 도용한 경험이 있는 경우는 응답자의 12%나 된다. 이 같은 결과는 인터넷상의 주민등록번호 도용이 일반인들 사이에서도 매우 빈번히, 아무렇지 않게 이뤄지고 있음을 입증하는 것이다.

둘째, 현재 대부분의 ID, PW 방식에서는 한사람의 ID, PW로 여러 명이 사용이 가능하다는 것이다. 이는 서비스 제공자에게는 크나큰 손실이 아닐 수 없다.

따라서 이러한 문제점들 보완하기 위해서 원격교육 시스템에서 인증 및 전자서명이 필수적

인 요소가 된다.

앞서 언급한 문제점들을 다시 정리해 보면 다음과 같다.

① 우선 기존 원격교육 시스템에서 ID, PW 방식으로의 문제(다수 이용 가능)

② 원격교육 시스템에서의 인증제도 존재여부 없음(공인인증서를 꼭 사용해야 한다는 의무화 없음)

③ 시스템에서 사용자들의 개인정보 보호가 잘 이루어지지 못하다는 점(보안성 및 신뢰성 없음)

④ 공인인증서의 유료화(앞으로 사용자들의 부담)

⑤ 공인인증서 검증방법인(인증서폐지목록) CRL, Delta CRL, OCSP방법은 CA산하에 있는 각종 금융은행 및 증권사를 묶고 있는 CA 및 RA에 인증서 유효상태를 매번 검색해야 하는 문제점(시간 및 네트워크의 Overhead 문제)

3. MCAS시스템(Multi-Certification of Agent System)

2장에서 제시한 원격교육의 문제점들을 해결하기 위하여 MCAS System을 제안하고자 한다.

3.1 시스템 구성

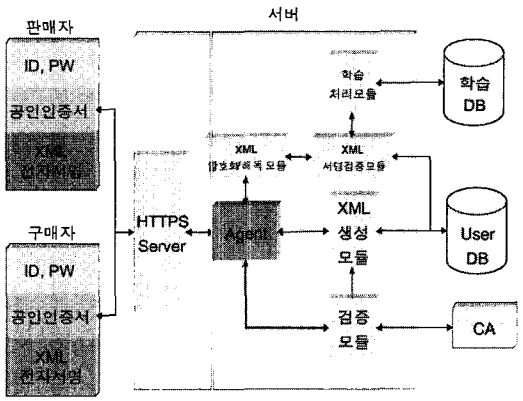
MCAS 시스템의 구성은 (그림 3-1)과 같다. MCAS 시스템은 사용자가 처음 가입할 때 Http Server를 통해 에이전트가 검증모듈을 거쳐서 CA를 통해서 인증서를 받아 처음으로 인증을 받는다.

인증이 확인된 사람들로만 회원 가입을 할 수 있게 된다.

회원 가입을 할 때 XML 생성 모듈에서 개개인의 XML 전자서명을 발급 한다. 따라서 다음부터는 CA를 통해서 인증서를 확인 할 필요 없이 발급 받은 XML 전자서명을 이용하면 된다. 이로 인해서 사용자 및 관리자는 공인인증으로 인한 처리 비용을 줄일 수 있다.

일단 한번 발급 받은 전자서명은 폐지가 가능하며 폐지가 되었다면 다시 발급받아야 하고, 기존의 XML 전자서명은 사용 못하게 된다.

새로 XML 전자서명을 발급 받을 시에는 다시 CA를 통해서 인증을 확인해야 한다.



(그림 3-1) MCAS시스템 구성도

3.2 역할 및 규칙

① Agent 모듈 - HTTP 서버를 통해 들어온 메시지 값을 각각의 모듈로 넘겨주는 모듈
(메일 푸쉬 기능 - 학습과제에 대한 가격 및 정보 제공, 문제 풀이에 대한 정보제공, 성적 비교 자료 등을 메일로 확인 가능)

② 검증 모듈 - 회원 가입시 CA에 공인인증서 유효상태 확인 모듈

③ XML 생성 모듈 - 회원 가입시 공인인증서가 정상적이면 XML 생성모듈에서 MCAS자체 XML 전자서명을 발급 모듈

④ XML 암호화/해독 모듈 - 사용자가 학습을 하기위해 접속 할 때 MCAS XML 전자서명을 해독하는 모듈

⑤ XML 서명검증모듈 - MCAS XML 전자서

명의 유효상태 확인 모듈

3.3 XML 전자서명

본 시스템에서 XML 전자서명의 역할은 다음과 같다.

① 위조불가 : 전자서명 생성 불가
② 변경불가(Message Authentication) : 개인키를 소유하지 않은 자는 전자문서 변경 불가
③ 서명자 인증(Signer Authentication) : 생성키를 소유한 자가 전자서명의 행위자임을 인증
④ 부인불가 : 전자서명 후 행위에 대한 부인 불가

MCAS는 처음 가입시에만 공인인증을 확인하기 때문에 RA 및 CA에 대한 과부하를 줄일 수 있고, Multi Agent 기술을 사용하기 때문에 사용자 및 관리자의 수작업 또한 줄어들게 된다.

그리고 자체 내의 XML 전자사명을 사용하기 때문에 다른 사용자의 ID와 PW를 알고 있어도 접근을 하지 못하며, XML 전자서명으로 인한 사용자들의 기밀성, 무결성 및 신뢰성이 보장된다. 또한 앞으로 공인인증을 받을 때 내야 할 비용 면에서 사용자 및 관리자의 비용절감을 가져다 줄 수 있다.

4. 결론 및 향후과제

본 논문은 XML 전자서명 기법을 이용한 다중인증 원격교육 에이전트 시스템을 제안하였다. 이는 앞으로 웹상에서 사용되어지는 공인인증서에 대한 소비자와 관리자의 금전적인 면에서 또한 사용자의 ID, PW로 인한 보안적 측면을 고려한 방법으로 XML 전자서명 기법을 이용한 다중인 방식을 추가 시키는 방법이다.

본 시스템을 적용시킴으로서 다음과 같은 효과를 얻을 수 있다.

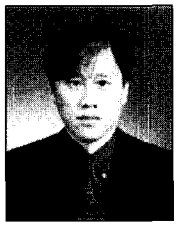
처리 속도 면에서 공인인증서만 사용하는 경우보다 XML 전자서명을 사용할 경우 처리 속도에 대한 향상을 가져올 수 있다. Network문제에서도 OCSP or CRL 보다 Overhead를 감소 할 수 있으며 Real-Time을 최대한 보장 받을 수 있다. 또한 사용자 측면에서는 부인방지 및 무결성, 기밀성, 신뢰성 보장을 가져오며 금전적 부담 면에서도 감소할 수 있다. 관리자 측면에서는 수작업으로 처리해야 할 문제들이 감소됨으로 Interface 향상을 가져 올수 있다고 본다.

향후 과제로는 전자상거래에 적합한 다중인증 에이전트 시스템에 대한 연구가 필요할 것으로 사료된다. 전자상거래에서는 구매자와 판매자가 존재하기 때문에 처음 한번의 CA를 통한 인증 후에 발생할 수 있는 신뢰성에 관한 문제점이 생길 수 있다. 따라서 제안된 다중인증 에이전트 시스템을 어떻게 설정하고 적용가능하게 할 것인가에 대한 연구가 필요하다고 본다.

참 고 문 헌

[1] Ray Hunt, "Technological Infrastructure for PKI and Digital Certification", 2001.
[2] Vishwa Prasad and Sreenivasa Potakamuri & Michael Ahern, "Scalable Policy Driven and General Purpose Public Key Infrastructure(PKI)", IEEE, 2000.
[3] Eugenio Faldella and Marco Prandini, "A Novel Approach to On-Line Status Authentication of Public-Key Certificates", *IEEE*, 2000.
[4] RFC3080, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile, 2002.
[5] draft-ietf-pkix-cvp-02, Certificate Validation Protocol, 2003.
[6] 김윤태, 김원영, 김치수, "원격 교육을 위한

WMPB의 설계와 구현", '98정보처리학회 추계학술대회, 1998.
[7] 김용호, 김희철, "웹 기반 정보처리 기능사 문제은행 시스템 설계 및 구현", 정보과학회 2003년 추계학술대회, 2003.
[8] 정재동, 오해석 "실시간 인증서 상태검증의 성능개선", 한국정보처리학회 논문지C, 2003.
[9] 황민구, "이종의 시스템에서 OCRS를 이용한 효율적인 인증서 상태 검증에 관한 연구", 정보과학회 추계학술대회, 2002.



김 귀 남

University of Kansas, U.S.A.(학사)
Colorado State University, U.S.A. (석사)
Colorado State University, U.S.A. (공학박사)
2000~현재 경기대학교 정보보호기술공학 교수
2001~현재 한국사이버테러정보전학회 회장
2001~현재 경찰청 사이버치안위원회 자문위원
2002~현재 KT 정보보안기술협의회 회장
2002~현재 국정원 국가정보보안협의회 위원