論文
6-3-9

WBI에서 XML 전자 서명을 이용한 다중 인증 시스템 설계 및 구현 (Design and Implementation of Multiplex Certification System Using XML Signature For WBI)

엄기원(Eom Ki Won)[1] 김정재(Kim Jung Jae)[2] 전문석(Jun Moon Seuck)[3]

요 약

정보통신 기술의 비약적인 발전으로 인해 인터넷은 필수 불가결한 도구가 되고 있다. 이러한 정보화 시대의 요구에 대한 교육적 대응은 학습자중심의 교육이며, 정보통신 기술을 기반으로 한 원격 교육이다. 그와 더불어 차세대 웹 표준문서 포맷으로 부상되고 있는 XML(eXtensible Markup Language)을 사용한 규격에 대한 국내외적인 표준화 작업 또한 가속화되고 있으며, 최근 XML 보안에 대한 연구가 활성화 되고 있다. 하지만 2004년부터 사용자들은 CA를 통해 인증을 받으려고 하면 인증서비스에 대한 지불을 해야 하는 단점이 있다. 본 논문에서는 기존의 원격교육 사이트에 다중인증 기법을 적용하여 가입시에 공인인증서를 한번 받도록 하며, 본 시스템에서 제안하는 XML 전자서명을 발급받아 보안성을 유지할 수 있는 방법을 제안하고 이에 대한 시스템 구현을 통해 해결하고자 한다.

ABSTRACT

Internet becomes absolutely necessary tools due to rapid progress of information technology. Educational correspondence abount an age of information demand is a education focused on a learner and remote education based on information technology. Internal and external standardization working is accelerated and recently XML security studies are activated using XML which is next generation web standard document format. But using these are main contents that users have to pay about Certification service to get CA certificate from 2004 june. This paper propose multiplex Certification remote education agent system using XML digital signature to satisfy security requirement.

논문접수 : 2005 7. 15.
심사완료 : 2005. 8. 10.

1) 정회원 : 숭실대학교대학원 컴퓨터학과 박사과정

2) 정회원 : 숭실대학교대학원 컴퓨터학과 박사

3) 정회원 : 숭실대학교 정보과학대학 정교수

1. 서 론

멀티미디어와 정보통신의 기술발전은 컴퓨터 환경에 많은 변화를 가져왔고, WWW(World Wide Web)의 등장으로 원격교육은 큰 전환점을 맞이하게 되었다. 이러한 추세는 PC통신 및 네트워크의 대중화에 따라 인터넷의 사용이 보편화되었으며, 이들 기술을 이용한 교육시스템들이 개발되어 활용되고 있다. 원격교육 분야에서도 WWW가 나오기 이전의 교육용 시스템들은 대부분 텍스트나 간단한 그래픽 기반으로 설계 개발되어 졌고, 이 시스템들은 단방향의 학습과 평가가 가능했을 뿐 양방향의 상호작용적 학습이 이루어지지 못했다. 하지만 WWW는 분산 환경을 제공함으로써 지역적으로 멀리 떨어져 있는 학습자가 실시간으로 양방향의 상호 작용적 학습이 가능해졌을 뿐만 아니라 실시간 학습과 평가를 가능하게 해주었다.

원격교육이란 용어는 외국에서도 Distance-education, Tele-education, Open-education 등과 같이 혼용되고 있으며, 원격교육은 떨어져 있는 학습자들에게 도달하기 위한 다양한 매체와 기술을 사용한 계획된 교수·학습경험으로 학습자 상호작용을 격려하고 학습을 인증하는 것이다[1]. 이런 원격교육을 하기 위한 보안 요소로써 현재 사용하는 기법은 공인인증서와 전자서명이 그 대표적이라 할 수 있다.

전자서명이란 상대방에게 송신자의 신뢰성을 증명해주는 방법이며, 임의의 공격으로 인한 문서 위조를 방지하기 위한 기법으로, 상대방에게 전자적으로 작성된 서명이 첨부된 형태의 문서를 전송하여 수신자로 하여금 확인 가능하게 하는 것이다. 다목적용 공인인증서의 시행으로 인해 유료화 되었으며, 은행에서 발급하는 개인의 인증서는 은행이 금융결제원에게 이미 분담금 형태로 인증 수수료를 받고 있다. 다목적용이란 인터넷 뱅킹은 물론 사이버 증권용, 카드용, 보험용, 전자정부 민간용, 일반 전자상거래용에 이르기까지 모든 분야에 쓸 수 있는 소위 범용 공인인증서를 말한다[6]. 또한 공인인증서는 1년마다 다시 발급받도록 되어 있으며, 만약 분실 시에도 다시 받아야 되므로 부담은 늘어갈 수밖에 없다. 또한 원격교육의 사용자들에 대한 ID, PW(Pass Word) 방식에는 한 사람의 ID, PW로 다수가 이용가능하다는 것과 해킹 등 많은 문제점들이 발생하고 있는 것이 현실이다.

따라서 본 논문에서는 기존의 원격교육 사이트에 다중인증 기법을 적용하여 가입시에 공인인증서를 한번 받도록 하며, 본 시스템에서 제안하는 XML 전자서명을 발급받아 보안성을 유지할 수 있는 방법을 제안하고 이에 대한 시스템 구현을 통해 해결하고자 한다.

본 논문의 2 장에서 WBI 개요 및 XML 전자서명에 관련된 연구와 원격교육 시스템의 문제점에 대해서 함께 개괄적으로 언급을 하고 제 3 장에서는 XML 전자서명을 이용한 다중인증 시스템의 전체적인 구조와 구성요소들의 역할 및 규칙에 대하여 살펴본다. 제 4 장에서는 본 논문의 가장 핵심이 되는 부분의 XML 전자서명 구현과정 및 내용에 대해서 설명하고, 마지막으로 제 5 장에서는 본 연구의 결과를 바탕으로 결론을 논하고, 아울러 앞으로의 연구 방향에 대해 기술한다.

2. 관련 연구

2.1 WBI(Web Based Instruction)

오늘날 인터넷에 접속할 수 있는 가장 쉽고 가장 인기 있는 방법인 WWW의 등장과 함께 인터넷은 가장 중요한 교수도구로서 교사들에게 인식되고 있으며, Web을 이용한 새로운 교수모형에 대하여 시각이 집중되고 있다. 새롭게 출현하고 있는 이 교수모형을 WBI이라고 부르고 있는데, 이는 특정한 그리고 미리 계획된 방법으로 학습자의 지식이나 능력을 육성하기 위한 의도적인 상호작용을 Web을 통해 전달하는 활동이라고 정의 내릴 수 있다. 설계가 잘 된 WBI는 어떠한 주제에서건 학습자 주도적(self-directed)이고 학습자의 속도에 맞는(self-paced) 교수법을 제공하며, 다양한 매체 중심의 교육을 제공하기 위해 Web Browser

와 대중들의 인터넷 접속을 확대시킨다는 장점을 지니고 있다. WBI의 발달은 컴퓨터 네트워크 공학의 발전과 그것의 교육적 활용에 그 바탕을 두고 있다고 볼 수 있다. 컴퓨터 네트워크가 교육에 활용된 형태는 크게 세 가지 정도로 구분되어 진다.

첫째로, 컴퓨터 네트워크가 면대면 교육이나 원격교육 등에서 하나의 보조적 매체로 활용되는 형태가 있으며, 둘째로는 컴퓨터 네트워크가 전체 강좌나 강좌의 일부를 가르치는 주된 매체로 활용되는 형태가 있다. 세번째 형태로는 컴퓨터 네트워크를 보다 자유로운 지식 네트워킹의 장, 토론에의 참여 수단, 온라인 데이터베이스 활용의 수단, 또는 세계에 흩어진 전문가나 동료들과의 정보교환의 수단 등으로 이용하는 형태이다.

이러한 WBI 시스템에서는 많은 발전이 있지만 시스템의 보안적 측면에서는 다수의 관리자 및 이용자들의 보안의식이 많이 부족한 실정이다. 인터넷 강국의 입장에서 많은 보안사고가 발생하고 있는 것이 현실이며 이는 국가의 신용 및 신뢰도를 크게 떨어뜨릴 수 있는 것이다. 또한, 기존 WBI에서는 보안에 관한 부분이 구체적으로 고려되지 않았다. 따라서 본 논문에서는 기존의 원격교육 사이트에 다중인증 기법을 적용하여 보안성을 유지할 수 있는 방법을 제안한다.

2.2 전자 서명

전자서명(Digital Signature)은 공개키(Public Key) 방식을 사용하여 사용자 인증과 메시지 불변성을 보장 해주는 기술이다. 공개키 방식이란 사용자마다 자신만이 알고 있는 개인키(Private Key)와 이에 대응되면서 다른 사람들에게 알려줘야 하는 Public Key, 한 쌍의 키들을 암호화와 복호화에 사용하는 것이다. 이 때 Private Key를 사용하여 메시지를 암호화한 경우 Public Key를 사용하여야 해독할 수 있고, 반대로 Public Key를 사용하여 암호화 한 경우는 대응되는 Private Key를 사용하여야 해독 가능하다. 전송하고자 하는 상대의 Public Key로 메시지를 암호화한 경우에는 원하는 상대만이 자신의 Private Key를 사용하여 해독할 수 있으므로 메시지 내용의 기밀성이 필요한 경우에 사용된다. 반대의 경우, 즉 자신의 Private Key로 암호화한 경우에는 공개되는 Public Key로 누구나 해독할 수 있으므로 내용의 기밀성 보다는 메시지의 작성자를 인증하고 메시지 내용의 불변성을 인증하는 데에 사용되며, 이를 전자서명이라 한다.

2.2.1 XML 전자서명

XML의 초창기에는 보안 관련 요소를 자체적으로 정의하지 않았지만 XML의 이용범위가 확대됨에 따라 암호화와 전자서명, 키 관리 등을 위한 XML 표준이 제정되고 있으며, 현재 몇 개의 참조구현과 상용 라이브러리가 출시된 상태다. 또한 XML을 활용한 문서 교환시의 보안에 대한 표준화 작업 또한 활발히 진행되고 있다. 기존의 보안과 비교하여 XML 보안이 가지는 장점은 다음과 같다.

① 기존의 XML의 장점인 문서 자체 내에서의 구조적인 정보를 활용하여 전자 서명을 일부 혹은 문서 전체에 적용시킬 수 있다.
② Namespace를 사용할 수 있다.
③ XML 보안을 활용하여 원격교육 시스템을 한층 더 촉진 시킬 수 있다.

<표 1>은 XML 전자서명 문법의 기본 구조를 보여주고 있다.

① <Signature> : XML 서명문서의Root 엘리 먼트
② <SignedInfo> : 서명될 요소들에 해당.<CanonicalizationMethod> :서명 값을 수행하기 전 단계에 해당, XML문서를 정규화하기 위해 필요로 되는 알고리즘.
③ <SignatureMethod> : 서명 값을 발생하기 위해 사용되는 알고리즘을 제공 (DSAwithSHA1, RSAwithSHA1)
④ <Reference> : id를 통해 다른 곳에서 참조됨. 메시지다이제스트알고리즘, 메시지의 다이제스트 값, Transforms 엘리먼

트 포함가능

⑤ <Transforms> : 서명자가 메시지 다이제스트 객체를 얻는지를 묘사. 메시지다이제스트알고리즘은SHA-1사용, Base 64를 기반 코딩 방식.

⑥ <DigestMethod> : SHA-1사용

⑦ <KeyInfo> :키에 대한 정보를 입력. 키, 이름, 인증서 및 다른 공용키 관리 정보를 포함

<표 1>] XML 전자서명 문서의 기본 구조

```
<Signature>
  <SignedInfo>
   (CanonicalizationMethod)
   (SignatureMethod)
   (<Reference (URI=)? >
      (Transforms)?
      (DigestMethod)
      (DigestValue)
   </Reference>)+
  </SignedInfo>
  (SignatureValue)
 (KeyInfo)?
 (Object)*
</Signature>

1. "?" = zero or one occurrence
2. "+" = one or more occurrences
3. "*" = zero or more occurrences
```

2.2.2 전자서명 인증

전자서명 인증이란 전자서명 검증키가 자연인 또는 법인이 소유하는 전자서명 생성키에 합치한다는 사실을 공신력 및 전문성을 갖춘 인증기관이 확인·증명하는 행위를 말한다. 인증기관은 이를 위하여 서명자, 전자서명 검증키 등의 정보가 포함된 전자적 인증서를 발급한다.

최근 자주 언급되고 있는 인증은 일반적으로 크게 두 가지 의미로 나뉘어 사용되고 있다. 첫 번째는 사용자 인증이나 메시지 인증을 의미하는 인증(Authentication)이고, 두 번째는 공개키 암호방식에서 공개키 무결성의 보장을 의미하는 인증(Certification)이다. 물론 일각에서는 보증(Certification)이라고 정의하여, 인증(Authentication)과 구별을 하기도 하지만, 일반적으로 혼용되고 있는 상태이며, 여기서 언급하는 인증서비스는 인증(Certification) 서비스를 의미하며, 이것은 인증(Authentication)과는 구분된다. 전자서명은 Electronic Signature와는 다른 Digital Signature를 의미한다.

Electronic Signature는 도장이나 수기서명을 이미지(Image)화하여 저장하였다가 서명 시점에 사용하는 것으로서 복제가 쉬우며 시각에 의한 확인으로 진위여부를 판단하기 때문에 전자서명이라 할 수 없다. 이에 비해 Digital Signature는 컴퓨터에 의해 복잡한 수학적 연산을 통해 서명 값을 생성 하는 것으로서, 대상이 되는 정보가 달라짐에 따라 생성되는 값도 달라지게 되므로 복제가 불가능하며, 전자서명 생성키를 소유한 당사자만이 서명 값을 생성할 수 있기 때문에 타인에 의한 임의의 서명도 불가능하다. 서명 값의 진위여부 또한 컴퓨터를 사용하여 수학적 연산 을 통해 이루어지기 때문에 Digital Signature를 전자서명이라고 한다.

1) 인증서 폐지 목록
(Certificate Revocation List : CRL)

현재 사용되고 있는 인증서는 CCITT에서 제정한 X.509 V3이다. 인증서 유효기간은 인증서 발급일로부터 1년이며 USER에 개인키가 노출 되었을 때, 상위 CA의 비밀키가 노출 되었을 때, USER가 인증서를 발행했던 조직으로부터 퇴직 했을 경우와 같이 몇 가지 이유로 인해 인증서 유효기간 이전에 폐지 될 수 있다. 위와 같이 폐지된 인증서가 불법적으로 사용되거나 도용되는 것을 막기 위해 폐지된 인증서를 하나의 리스트로 모아놓은 것이 CRL이다 [2, 7]. 하지만 CRL은 인증서의 발급이 증가할수록 폐지되는 인증서의 양도 증가하기 때문에 CRL을 보관하기 위한 파일에 크기 또한 기하급수적으로 증가한다는 단점과 하루에 한 번씩 인증서 폐지 목록을 다운 받기 때문에 실

시간으로 인증서 상태를 검증할 수 없다는 단점이 있다[7].

2) OCSP

OCSP는 CRL기반의 인증서 검증 방식에 문제점인 인증서에 대한 실시간 상태 검증을 해결하기 위해 제안된 인증서 상태 검증 방식으로 1999년 6월 IETF RFC2560문서에 의해 공포되었다[8]. OCSP 인증서 상태 검증 방식은 USER가 CA로부터 인증서를 발급받은 후 USER가 정해진 포맷으로 OCSP 클라이언트에게 전자서명을 요청하면 OCSP 클라이언트는 정해진 포맷으로 OCSP 서버에게 인증서 상태를 요청하고, OCSP 서버는 요청받은 인증서에 대한 상태 정보를 검색하여 전자서명을 수행한 후 수행결과의 대한 응답을 OCSP 클라이언트로 넘겨줌으로써 실시간으로 인증서에 대한 유효성 검사를 수행하는 방식이다[8, 9].

OCSP 기반의 인증서 검증 방식은 OCSP 클라이언트가 CRL을 요청하지 않고 인증서의 현재 상태를 검증하기 때문에 실시간으로 인증서에 대한 상태검증을 할 수 있다는 장점이 있는 반면 실시간으로 인증서에 대한 유효성 검사를 수행해야 하기 때문에 많은 통신량으로 인한 네트워크 과부하 문제를 발생시킨다는 단점과 네트워크 상태의 따라 인증서 유효성 검사의 수행시간이 달라진다는 단점이 있다.

2.2.3 기존 연구의 문제점 및 해결책

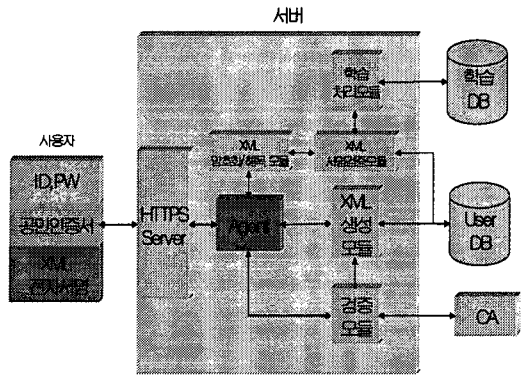
① 우선 기존 원격교육 시스템에서 ID, PW 방식으로의 문제(다수 이용 가능)
② 기존 원격교육 시스템에서의 인증제도 존 electronic signature와 digital signature의 차이재여부 없음(공인인증서를 꼭 사용해야 한다는 의무화 없음)
③ 기존 시스템에서 사용자들의 개인정보 보호가 잘 이루어지지 못하다는 점(보안성 및 신뢰성 없음)
④ 공인인증서의 유료화(사용자들 부담이 늘어남)
⑤ 기존 공인인증서 검증방법인(인증서폐지목록) CRL, OCSP방법은 CA산하에 있는 각종 금융은행 및 증권사를 묶고 있는 CA 및 RA에 인증서 유효상태를 매번 검색해야 하는 문제점(시간 및 네트워크의 Overhead 문제)

이와 같이 기존 원격교육 시스템 및 기존 연구 분석의 결과 많은 문제점들이 발견되었다. 또한 앞으로 정부에서 공인인증서를 인터넷서비스 전반으로 확대해 가고 있으며 원격교육 시스템에서의 공인인증서의 필요성을 위에서 살펴보았다.

그러나 공인인증서 사용의 실시간성 문제점과 공인인증서의 유료화로 인한 사용자들의 부담을 고려하고, 다른 여러 문제점들을 이 논문에서는 다중인증 시스템을 사용하여 해결하는 방법으로 제안한다.

3. 다중 인증(Multiplex Certification Agent System) 시스템 설계

3.1 MCAS 시스템 설계



(그림 1) MCAS 시스템 구성도

(그림 1)은 사용자와 시스템 서버간의 구조로 MCAS의 전체적인 구조를 나타내고 있다.

① Agent 모듈 : HTTP 서버를 통해 들어온 메시지 값을 각각의 모듈로 넘겨주는 모

듈이다. 회원 가입을 하는 사용자는 개인의 정보를 입력하여 처음으로 CA를 통한 인증 확인 절차를 거치게 한다.

② 검증 모듈 : 개인 사용자의 공인인증서를 검증하는 모듈로 회원 가입시 CA에 공인인증서 유효상태 확인 모듈이다. 본 논문에서는 공인인증서의 유무로써 이 부분을 대신하여 처리하였다.

③ XML 생성 모듈 : 회원 가입시 공인인증서가 정상적이면 XML 생성모듈에서 MCAS자체 XML 전자서명을 발급하는 모듈이다. 회원가입 시에 올바른 공인인증을 확인된 사용자에 대해서 개인별 XML 전자서명을 사용자 및 시스템 DB에 발급하여 저장한다.

④ XML 암호화/해독 모듈 : 사용자가 학습을 하기위해 접속 할 때 MCAS XML 전자서명을 해독하는 모듈이다. 암호화된 개인별 XML 전자서명을 해독하는 모듈이다.

⑤ XML 서명검증모듈 : MCAS XML 전자서명의 유효상태 확인 모듈이다. 해독된 전자서명과 DB에 저장된 전자서명을 비교하여 올바른 것인지를 검증하는 모듈이다.

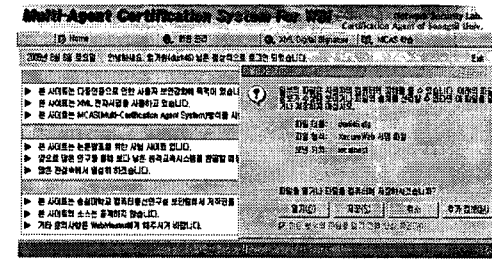
4. MCAS 시스템 구현

4.1 시스템 환경

시스템의 구현에 사용된 하드웨어로는 윈도우즈 NT 2000 Advenced Server가 탑재된 펜티엄III PC가 사용되었다. XML 전자서명 생성과 검증을 위해 IBM사의 XSS(XML Security Suite)를 사용하였다. 프로그램을 위한 언어로는 마이크로소프트사의 ASP 3.0, 자바 애플릿, JDK 1.4.2를 사용하였다.

4.2 XML 전자서명 다운로드

회원 가입시 CA를 통해 인증을 확인 사람에 한하여 MCAS 시스템 자체에서 개인별 XML 전자서명을 부여한다. (그림 2)는 올바른 인증을 통해 회원가입을 통과하였을 때 이후 XML 전자서명을 다운받는 것을 보여주고 있다.



(그림 2) XML 전자서명 다운로드

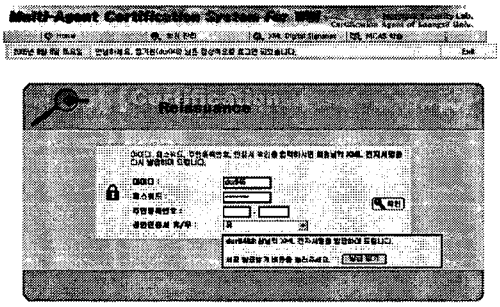
또한 (그림 3)은 개인에게 부여된 XML 전자서명의 내용을 보여주는 것이다.

```
<?xml version="1.0" encodin
- <Signature xmlns="http://v
  - <SignedInfo>
      <CanonicalizationMethod
      <SignatureMethod Algor
    - <Reference URI="#Res0
        <DigestMethod Algorit
        <DigestValue>vJw1jc
      </Reference>
    </SignedInfo>
    <SignatureValue>dMbqpR
```

(그림 3) 개인에게 발급된 XML 전자서명

4.3 XML 전자서명 재발급

본 시스템을 사용하기 위해서는 ID, PW, 개인 XML 전자서명이 필요하므로 전자서명을 분신하였거나 어떤 잘못으로 인해서 재발급을 받아야 할 때 (그림 4)를 통해서 재발급을 신청해야 한다.

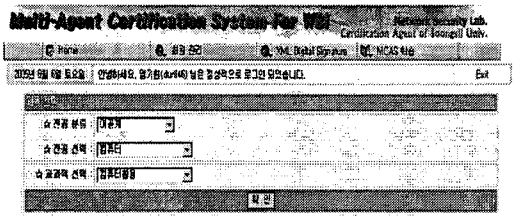


(그림 4) XML 전자서명 재발급 처리 화면

재발급시에도 본인의 확인 과정을 거쳐야 하므로 ID, PW, 주민등록번호, 그리고 공인인증서확인을 한 후에 다시 새로운 XML 전자서명을 다운받을 수 있다. 또한 새로 받은 전자서명 외에 기존의 전자서명을 가지고는 시스템에 접근은 할 수 없게 된다. 그리고 ID, PW를 기억하지 못하는 경우 XML Digital Signature에서 ID, PW 확인을 클릭하여 주민등록 번호로 ID와 PW를 확인할 수 있다.

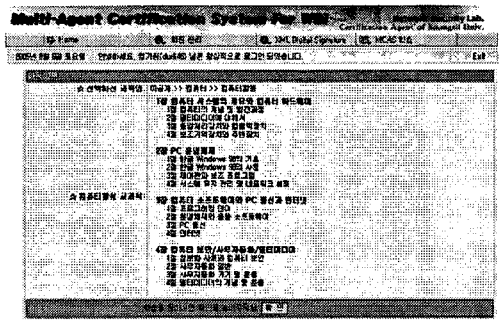
4.4 MCAS 학습방법

본 시스템에서는 전공분류별, 전공 선택, 교과목 선택으로 분리하여 사용자의 취향에 맞는 학습을 선택할 수 있게 하였다. [그림 5]는 MCAS 학습을 클릭 했을 때의 화면을 보여주는 것이다.



(그림 5) 학습등록 화면

(그림 6)은 학습등록 화면에서 자신이 선택한 과목에 대한 목차를 보여줌으로써 선택을 다시 할 수 있게 보여 주고 있다. 만약 선택한 과목의 내용이 사용자의 학습에 맞는 내용이 아닐 경우를 대비해서 확인 과정을 다시 거치는 화면을 보여 주고 있는 것이다. 선택 과목의 목차가 사용자의 학습 목표와 맞을 경우 확인을 누른 후 학습을 시작하도록 설계하였다.



(그림 6) 선택한 과목 목차 화면

또한 사용자의 XML 전자서명을 복사하여 다수가 사용하는 것을 막기 위해 학습 페이지를 하나의 ID로 5번 이상 접근을 할 수 없게 하였다.

5. 결론

본 논문에서는 다중인증을 사용하여 WBI에서의 보안을 강화시킨 MCAS (Multiplex Certification Agent System) 시스템을 제안하였다. 기존의 원격교육 시스템에서는 없었던 인증 방식을 접목시킨 것이 가장 큰 특징이며 공인인증서의 유료화로 인한 문제점을 해결하고자 다중인증 방식을 사용하였다. 또한 기존의 ID, PW 방식에서의 동일 ID, PW로 다수 사용가능 했던 것을 막으면서 전자서명을 사용함으로써 생기는 신뢰성 및 보안성을 강화 시켰다. 처리속도 면에서 공인인증서만 사용하는 경우보다 XML 전자서명을 사용할 경우 처리속도에 대한 향상을 가져오며, Network Overhead 감소로 인한 최대한의 Real-Time을 보장하며, 사용자 측면에서 부인방지 및 무결성, 기밀성, 신뢰성 보장과 함께 보안성을 강화 시켰다. 또한 공인인증서로만 사용했을 때의 금전적 부담 감소를 가져오며, Interface 향상을 추구하였다.

향후 연구는 다중 인증 에이전트 시스템을 전자상거래에서 적용시킬 때 관한 문제들을 연

구할 계획이다. 전자상거래에서는 구매자와 판매자가 존재하기 때문에 처음 한번의 CA를 통한 인증 후에 발생할 수 있는 신뢰성에 관한 문제점이 생길 수 있기 때문이다. 따라서 어떻게 설정하고 적용가능하게 할 것인지를 분석해 보려하고 또한 앞으로 공인인증서가 확대되었을 경우 회사규모나 학교에서도 본 다중인증 에이전트 시스템을 사용하는데 있어서 연구로 발전해 나갈 것이다.

참고 문헌

[1] 김윤태, 김원영, 김치수(1998), "원격 교육을 위한 WMPB의 설계와 구현", 98정보처리학회 추계학술대회

[2] 김현철, 이옥경, 이용준, 오해석(2003), "인증서 검증 시스템의 검증시간 비교분석에 관한 연구", 정보과학회 2003년 춘계학술대회

[4] 정재동, 오해석(2003), "실시간 인증서 상태검증의 성능개선", 한국정보처리학회 논문지 C,

[5] 황민구(2002), "이종의 시스템에서 OCRS를 이용한 효율적인 인증서 상태검증에 관한 연구", 정보과학회 추계학술대회,

[6] 신홍식(2005), "유료화 논쟁속 국내 공인인증 산업 기술의 현 주소", 한국정보과학회, VOL. 23 NO. 1 pp. 0015 ~ 0020

[7] J. Willemson(1998), "Certificate Revocation Paradigms", Technical Report, Cybernetica

[8] M.Myers, R.Ankney, A.Malpani, S.Galperin, and C.Adams(1999), "Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol-OCSP", RFC2560

[9] M.Myers, R.Ankney, C.Adams, S.Farrell and C.Covey(2001), "Online Certificate Status Protocol, Version2", draft-ietf-pkix-ocspv2-02

[10] RFC3080, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile, 2002

엄 기원

1981년 2월 : 덕성여자대학교 경영학과 학사

2000년 8월 : 숭실대학교 컴퓨터교육학과 석사

2001년 9월 ~ 현재 : 숭실대학교 대학원 컴퓨터학과 박사과정

2005년 9월 현재 : 부명정보산업고등학교 교사로 재직중

<관심분야> 네트워크 보안, 정보보안, 암호이론, 침입탐지

김 정 재

1995년 2월 : 영동대학교 컴퓨터공학과 학사

1999년 2월 : 숭실대학교 대학원 컴퓨터학과 석사

2005년 8월 : 숭실대학교 대학원 컴퓨터학과 박사

<관심분야> 멀티미디어 보안, 멀티미디어 데이터베이스, DRM, RFID 보안

전 문석

1980년 2월 : 숭실대학교 전자계산학과 학사

1986년 2월 : University of Maryland 전산과 석사

1989년 2월 : University of Maryland 전산과 박사

1989년 : Morgen State University 전산수학과 조교수

1989년 ~ 1991년 : New Mexico State University 부설 Physical Science Lab. 책임연구원

1991년 ~ 현재 : 숭실대학교 정보과학대학 정교수

<관심분야> 네트워크 보안, 컴퓨터 알고리즘, 암호학