XML-Signature 확장을 통한 2단계 서버 로그인 인증 시스템의 설계 및 구현

김 용 화[†] · 김 진 성[††] · 김 용 성[†††]

요 약

다양한 웹 콘텐츠 제공 환경에서 네트워크에 공개된 서버의 정보 자원을 보호하기 위하여 XML 보안 기술 스펙인 XML-Signature 스키마를 확장하여 2단계 서버 로그인 인증 시스템을 제안하고, 이를 설계 및 구현한다. 제안할 인증 시스템은 XML 기반의 인증서를 온라인상에서 요청 및 발행하고 인증기관에서 제공한 인증서확장 정보를 XML 인증서 관리 서버(XCMS)에 등록 한 후 사용자의 인증서 패스워드로 인증기관에 의해서 1차 인증을 수행한다. 또한 인증서 패스워드 이외에 추가로 입력한 인증서확장 정보와 인증서 관리서버에 등록된 사용자의 인증서 확장 정보를 SOAP 메시지로 요청한 후 두 값을 비교하여 2차 인증을 수행하는 보안이 강화된 인증 시스템이다.

키워드 : 서버보안, XML-Signature, SOAP, X509 v.3 인증서, 공개키 기반구조

A Design and Implementation of Two-Phase Server Login Authentication System based on XML-Signature Extension

Yong Hwa, Kim[†] · Jin Sung, Kim[††] · Yong Sung, Kim[†††]

ABSTRACT

This paper proposes a two-phase server login authentication system by XML-Signature schema extension to protect server's information resources opened on network which offer various web contents. A proposed system requests and publishes XML-based certificate through on-line, registers certificate extension information provided by CA(Certification Authority) to XCMS(XML Certificate Management Server), and performs prior authentication using user's certificate password. Then, it requests certificate extension information added by user besides user's certificate password and certificate extension information registered in XCMS by using SOAP message, and performs posterior authentication by comparing these certificate extension information. As a result, a proposed system is a security reinforced system compared with existing systems.

Key Words : Server Security, XML-Signature, SOAP, X509 v.3 Certificate, PKI

1. 서 론

오늘날 무선 인터넷에 관련된 기술의 향상과 해킹 기술의 발전으로 인하여 개인 및 기업 그리고 국가에 대한 정보 자산이 손쉽게 유출되고 파괴되는 경우가 빈번하게 발생되고 있다. 또한 여기에 대한 보안 기술과 솔루션 개발 역시 활발하게 진행되고 있는 것은 분명한 사실이다. 하지만 기존에 개발된 보안 솔루션은 시스템에 대한 호환성이 부족하고 시스템 간 연동이 곤란한 경우가 발생하여 효율성이 떨어지거나 유명무실화 되는 경우가 많다[1][4].

본 논문에서는 XML Signature 스키마를 확장하여 2단계 인증을 통해서 로컬 서버에 접속을 허용하기 위해 XCMS (XML Certificate Management Server)와 XCAS(XML Certificate based Authority Server)모델을 제안한다. 제안할 모델은 X509 v.3 유·무선 인증서를 온라인을 통해서 요청 및 발행하고, 발행된 인증서를 등록 및 조회 서비스를 제공하는 XCMS를 구축한 다음 인증기관으로부터 사용자에 대한 인증서 및 인증서 상태를 조회할 수 있는 XCAS에 메시지를 허용하여 접속자의 인증서 상태에 따라 로컬 서버 접속 여부를 결정하는 인증 시스템이다. 이를 위해 인증기관에서 발행된 인증서확장 정보를 XCMS에 등록하기 위한 요청 및 응답 메시지와 XCAS에서 XCMS에 인증서를 조회하기 위한 요청 및 응답 메시지는 SOAP(Simple Object Access Protocol)에 의해서 표현된다. 기존의 인증서 요청을

† 준 회 원 : 전북대학교 대학원 전산통계학과 박사과정
†† 준 회 원 : 전북대학교 대학원 컴퓨터통계정보학과 이학박사
††† 종신회원 : 전북대학교 전자정보공학부 교수
논문접수 : 2007년 3월 201일, 심사완료 : 2007년 8월 13일

위한 OCSP(Online Certificate Status Protocol)의 문제 해결 방안으로 SOAP 메시지를 사용하여 플랫폼에 독립적으로 서버 접속을 허용하도록 하였다[8].

따라서 본 논문에서는 XML-Signature 스키마를 확장하여 2단계 서버 로그인 인증 시스템을 설계 및 구축하여 XML 특성을 활용한 시스템간의 원활한 상호 연동과 인증서 패스워드 이외에 추가로 인증서확장 정보를 입력하게 하여 기존의 인증서 패스워드만의 입력 방식에 대해서 더 한층 안전성을 보장하는 서버 보안 모델을 제안하는데 목적이 있다.

본 논문의 구성은 제 2장에서는 관련연구로서 XML 기반의 보안기술에 관한 기존 연구와의 비교 분석 및 XML-Signature의 스키마와 SOAP 메시지의 구조에 대해서 알아본다. 그리고 제 3장에서는 제안할 시스템을 설계하고 제 4장에서 구현한 결과와 기존 연구와의 비교 평가를 논하고 마지막으로 제 5장에서 결론을 맺는다.

2. 연구배경 및 기반 기술

2.1 관련연구

본 논문은 웹에서 거래를 증명하고 신원을 확인하기 위한 XML 기반 전자서명 기법과 인증서 로그인 강화기법을 적용하여 2단계 인증을 수행하는 인증 시스템을 제안한다. 이 절에서는 제안할 인증 시스템을 설계 및 구현하는데 있어서 창의성과 독창성을 반영하기 위해 연구의 배경이 되는 관련 연구들을 분석한다.

먼저 서버 보안에 관한 연구들은 [2]와 [7]이 있다. [2]는 식별정보를 이용하여 서버공격으로부터 야기되는 위험을 감소시키는 서명 시스템을 제안하였고, [7]은 패스워드 기반 로밍 시스템에서 사용자의 해쉬 값으로 사용자를 인증하는 방법을 제안하였다. [2]의 연구에 대한 특징을 정리하면 자신의 고유 식별정보와 보안코드를 결합하여 개인키를 생성하기 때문에 서버 보안의 새로운 메커니즘을 제공하는 측면에서는 우수성을 보이지만 다양한 응용분야에서는 비교적 확장성이 낮은 특징을 보이고 있다. [7]은 패스워드 강화기법으로 해시 값을 적용하기 때문에 전자상거래 및 서버 보안 분야에 포괄적으로 적용이 가능하지만 기존에 제안한 XML 기반 보안 기법과 큰 차이가 없다고 볼 수 있다. 따라서 본 논문에서는 이러한 분석 결과를 토대로호환성 및 안전성을 고려한 새로운 인증서 로그인 강화기법을 제안한다.

또한 XML 전자서명 기법에 관한 연구에는 [1][8][11]이 있다. [1]은 전자상거래를 위한 비대칭 키 전자서명 기법의 정보통신 프로토콜에서 거래 당사자들 간에 전송된 메시지에 대한 책임 소재 증명의 분석을 위해 제안된 Kailar 책임 로직을 대칭키 암호화 기법의 전자서명을 사용하는 프로토콜에 적용하기 위해 일부의 구성 요소를 변경 및 추가하여 확장하였다.

[8]은 이기종간의 시스템에서 동작 가능하고, XML 문서를 보호할 수 있는 보안 메커니즘으로 XML-Signature를 설계하고 구현하였다. 즉, 웹 서비스 보안에 관한 연구를 기반으로 서비스의 호출을 담당하는 SOAP 메시지에 XML-Signcryption을 적용하여 보안 서비스를 제공하는 기법을 제안하였다.[11]은 XML-Signature와 XML-Encryption에 대한 스키마 예문과 하위 엘리먼트에 대해서 상세하게 기술하고 있다. 이와 같은 XML 전자서명 기법에 관한 연구 중에서 특히 [8]과 [11]에서 제안한 XML-Signature와 SOAP 메시지에 대한 활용 기법은 본 논문에서 응용 및 활용하였다.

2.2 XML-Signature

XML-Signature[14]는 사이버 상에서 거래를 증명하거나 신원확인이 필요할 때 이를 확실히 증명해주는 증명 수단으로 사용된다.

(그림 1)은 W3C 권고안에서 발표한 XML-Signature 엘리먼트[14]의 구성요소이다. <Signature>엘리먼트는 반드시 요구되는 필수사항 부분과 선택사항으로 사용되어지는 선택사항 부분 "( )"으로 나누어진다. <Signature>의 구성요소는 전자서명을 연산하기 위한 각종 알고리즘과 전자서명의 대상을 포함하는 <SignedInfo>와 실제 전자서명 값을 포함하고 있는 <SignagureValue> 그리고 전자서명 키(공개키) 정보와 X.509 인증서를 포함하고 있는 <KeyInfo>로 구성된다.

```
<Signature id ?>
  <SignedInfo>// 서명에 대한 실제 정보
    <CanonicalizationMethod/>//canonicalize하기위해 사용되어지는 알고리즘
    <SignatureMethod/>// canonicalize된 signedInfo를 SignatureValue로 치환하기
                         위해 사용하는 알고리즘
   (<Reference URI ?>
     (<Transforms/>)? // 서명자가 메시지 다이제스트 객체를 어떻게 얻는지 명시
      <DigestMethod/> // DigestValue를 산출하기 위해 적용할 알고리즘
      <DigestValue/>
    </Reference>)+
  </SignedInfo>
  <SignatureValue> // 디지털 서명의 실제적인 값, base64
 (<KeyInfo>)? // 키 발생기를 통해 생성되는 키에 대한 정보
 (<Objectid?>)*// 데이터 객체를 포함하기 위한 엘리먼트
</Signature>
```

(그림 1) XML-Signature Element 구성요소

2.2.1 SignedInfo 엘리먼트

<SignedInfo> 엘리먼트는 서명정보가 규격화되는 알고리즘을 명시한 <CanonicalizationMethod> 엘리먼트와 서명을 위한 알고리즘을 명시하고 있는<SignatureMethod> 엘리먼트 그리고 서명 데이터를 압축하고 압축 결과를 포함하고 있는 <Reference> 엘리먼트로 구성된다. 또한 <SignatureValue> 엘리먼트는 <SignedInfo> 엘리먼트에서 계산된 서명을 포함하고 있다. (그림 2)는 <SignedInfo>와 <SignatureValue> 엘리먼트의 예제이다.

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3c.org/TR/2001/REC-xml-c14n-20010315#"/>
    <SignatureMethod Algorithm= "http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
    <Reference URI="http://www.w3.org/TR/2000/signature-example.xml">
      <DigestMethod/Algorithm="http://www.w3c.org/2000/09/xmldsig#sha1"/>
      <DigestValue> Zu0kjcgV3t5VZWWdlvZ79sjk </DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue> w5smjh45y/89VVd3dBAQ </SignatureValue>
</Signature>
```

(그림 2) SignedInfo 엘리먼트 예

2.2.2 KeyInfo 엘리먼트

<SignatureValue>에 기록된 서명(Signature)을 사용하기 위해 키 정보를 제공하는 엘리먼트로 KeyName, KeyValue, X509Data 엘리먼트로 구성되어 있다. <KeyName> 엘리먼트는 전자서명이나 암호화를 수행하는 사람이 수신자에게 공개키를 식별하기 위해 사용되는 문자열을 포함하며, <KeyValue> 엘리먼트는 전자서명을 확인하고 데이터를 복화화하며 키를 일치시키는데 필요한 공개키의 실제 값을 포함하고 있는 엘리먼트이다. 또한 <X509Data> 엘리먼트는 X509인증서에 관한 정보를 포함하고 있다. (그림 3)은 <KeyInfo> 엘리먼트의 예이다.

<X509Data> 엘리먼트를 구성하는 하위 엘리먼트들이 포함하고 있는 내용은 <표 1>과 같다.

```
<Signature>
  <KeyInfo>
    <KeyName> kimjs </KeyName>
    <KeyValue> Xa7u+eOyH5..</KeyValue>
    <X509Data>
      <X509IssuerName>CN=kimjs, C=KR...</X509IssuerName>
      <X509SerialNumber>1234567</X509SerialNumber>
      <X509SubjectName>Certificate A </X509SubjectName>
      <X509Certificate>MIICSTCCA...</X509Certificate>
    </X509Data>
  </KeyInfo>
</Signature>
```

(그림 3) KeyInfo 엘리머트 예

〈표 1〉 X509Data의 하위 엘리먼트의 내용

엘리먼트	내 용
X509IssuerName	X509 인증서 발행자
X509SerialNumber	X509 인증서 키 식별자
X509SubjectName	X509 인증서 제목
X509Certificate	X509 v.3 인증서 및인증서 폐기목록(CRL)

2.3 SOAP(Simple Access Object Protocol)

SOAP은 분산 환경에서 정보 교환을 위한 단순한 XML 기반 프로토콜로 플랫폼이나 운영체제에 독립적으로 다양한 스타일의 정보교환을 지원하는 프로토콜이다. SOAP의 기능은 서비스 요청자에 의해서 요청할 메시지를 전송하고, 서비스 제공자는 해당 함수를 호출하여 응답메시지를 보내는 기능을 한다.

2.3.1 원격 메소드 요청 SOAP Message

원격 서버의 해당 메소드를 호출하여 데이터를 처리하기 위한 원격 메소드 요청 SOAP Message는HTTP Body를 통해 SOAP 메시지가 전달된다. 따라서 요청 SOAP 메시지는 HTTP Header 부분과SOAP Envelope 부분 그리고 실제 메시지를 포함하고 있는 SOAP BODY 부분으로 구성되다. 원격 메소드 요청 SOAP 메시지에 대한 예는 (그림 4)와 같다.

SOAP Body 부분에서는 XML 형식의 교환 정보를 기술하는 부분으로 http://www.confirm.co.kr URI로 신원확인을 요청하기 위해 사용자의 ID와 Password를 포함하고 있는 SOAP 메시지이다.

```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <a:authentication xmlns:a="http://www.confirm.co.kr">
      <a:ID> kpjiju </a:ID>
      <a:password> ****** </a:password>
    </a:authentication>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(그림 4) 원격 메소드 SOAP 메시지 예

2.3.2 원격 메소드 응답 SOAP 메시지

원격 서버의 XML 형식의 교환 정보가 전송되어 해당 메소드에 의해 처리된 결과를 요청한 사용자에게 응답하기 위한 원격 메소드 응답 SOAP 메시지는 (그림 5)와 같다.

SOAP Body 부분의 <auth_code>는 사용자 ID와 Password를 확인한 결과 값으로 "인증 확인 코드"를 포함하고 있는 응답 메시지의 예이다.

```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
  <a:authenticationResponse xmlns:a="http://www.confirm.co.kr">
    <a:auth_code> Nfakji423fnasik </a :auth_code>
    <a:password>******</a:password>
  </a:authenticationResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(그림 5) 원격 메소드 응답 SOAP 메시지 예

3. 2단계 서버 로그인 인증 시스템 설계

2단계 로컬 서버 로그인 인증 시스템은 XML 유·무선 인증서를 기반으로 사용자가 서버에게 로그인할 경우 2단계 인증을 통해서 로컬 서버의 접속을 허용하기 위한 보안 모델이다. 즉, 사용자가 요청한 유·무선 인증서를 발급한 후 인증서확장 정보를 인증서 관리 서버에 등록하여 인증서 패스워드로 1차 인증하고, SOAP 메시지를 통해서 인증서확장 정보를 요청하여 2차 인증을 수행하는 보안 모델이다.

본 장에서는 제안할 인증 시스템의 구성도, 수행 알고리즘 그리고 XML Signature 스키마 확장 설계에 대해서 기술한다.

3.1 용어 정리 및 시스템 구성도

3.1.1 용어 정리

본 논문에서는 다음과 같은 용어를 사용한다.

- User, CA, XCAS, XCMS : 각 객체 식별자(접속자, 인증기관, 인증서 인증서버, 인증서 관리서버)
- CA_{pw} : 사용자 인증서 패스워드
- CA_{ex_input} : 인증서 패스워드 이외에 사용자가 입력한 인증서확장 정보(랜덤 발생)

- CA_{CRL} : 인증서 유효기간
- User_Login(CA_{pw} , CA_{ex_input}) : 서버 접속자 로그인 정보
- $CA_{\_ex\_info}$: XML Signature 스키마 확장을 통한 사용자 인증서확장 정보
- $CA_{res}(M)$: 인증기관의 인증서 등록 요청 메시지 (M=CA_{pw} , $CA_{\_ex\_info}$)
- $XCMS_{reg\_num}$: XCMS의 등록 시리얼 번호
- $XCMS_{res\_mess}$:XCMS의 결과 메시지
- $XCMS_{req\_CA}(M)$: 인증기관의 인증서 등록 요청 메시지에 대한 XCMS의 인증서 등록 요청 응답 메시지 (M=$XCMS_{reg\_num}$, $XCMS_{res\_mess}$)
- $XCAS_{res}(M)$: XCAS의 사용자 인증서확장 정보 요청 메시지(M=CA_{pw} , CA_{ex_input})
- $XCMS_{req\_XCAS}(M)$: 사용자 XCAS의 인증서확장 정보 조회 요청 메시지에 대한 XCMS의 인증서확장 정보 조회 요청 응답 메시지(M=CA_{pw} , CA_{CRL})

3.1.2 시스템 구성도

본 논문에서 제안하는 XML-Signature 스키마 확장을 통한 2단계 인증을 위한 서버 로그인 시스템의 전체 구성도는 (그림 6)과 같다.

2단계 로컬 서버 로그인 인증 시스템의 각 구성요소는 다음과 같다.

(1) 접속자(User)

로컬 서버에 접속하는 사용자로 2단계 인증이 필요한 주체이다. 따라서 다음과 같이 인증서 패스워드와 랜덤하게 발생된 인증서확장 정보를 입력한다.

User_Login(CA_{pw} , CA_{ex_input})

(2) 인증기관(CA: Certification Authority)

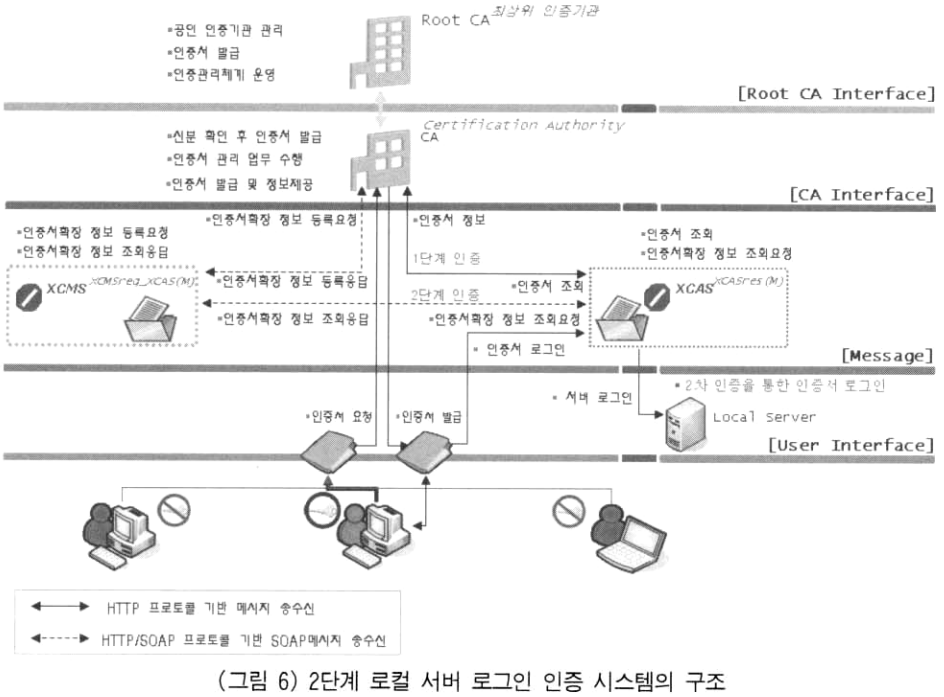
사용자에게 인증서를 발급하고 관리하며, XML-Signature의 <X509Items> 엘리먼트 확장을 통해서 얻은 인증서확장 정보를 XCMS에 등록하기 위해서 등록을 요청하는 신뢰기관이다.

- 인증서 발급 모듈
  사용자가 On-line상에서 인증서를 신청하면 보안 서버 인증기관에서 사용자의 신원확인 및 인증서를 발급한다.
- 인증서확장 정보 등록요청 모듈
  인증서 발급 모듈에 의해서 발행된 인증서확장 정보를 XCMS에 등록하기 위해서 다음과 같이 SOAP 메시지를 작성하여 등록을 요청한다.
  $CA_{res}(CA_{pw}$, $CA_{\_ex\_info})$

(3) XCMS(XML Certificate Management Server)

인증기관으로부터 인증서확장 정보를 전송받아 인증서확장 정보를 등록하고, 등록한 정보에 대해서 XCAS의 요청에 대한 응답 서비스를 제공하는 서버이다. 본 논문에서는 이를 XCMS라 명명한다.

- 인증서확장 정보 등록응답 모듈
  보안 서버 인증기관에서 발행된 인증서확장 정보(인증기관명, 일련번호, 허가코드, 가입날짜, 허가코드, 전자서명 알고리즘명, 가입자명, 주민등록번호)를 XCMS에 등록하기 위해서 다음과 같이 SOAP 메시지를 작성하여 등록 메소드를 호출하여 데이터베이스에 등록한다.
  $XCMS_{req\_CA}(XCMS_{reg\_num}$, $XCMS_{res\_mess})$
- 인증서확장 정보 조회응답 모듈
  XCAS에서 인증서 정보에 대한 조회가 요청될 경우 인증서 상태 조회 응답 모듈의 조회 메소드를 호출하여



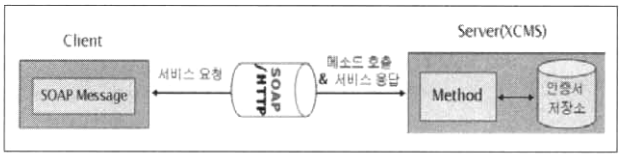
(그림 6) 2단계 로컬 서버 로그인 인증 시스템의 구조

다음과 같이 SOAP 메시지를 작성하여 요청한 인증서 확장 정보를 제공한다.

$XCMS_{req\_XCAS}(CA_{pw}, CA_{CRL})$

인증서확장 정보 등록 및 조회응답 서비스에 대한 메시지는 SOAP 형식을 따르며, SOAP 메시지에 대한 수행 과정은 (그림 7)과 같다.

Server는 인증서확장 정보를 등록하고 인증서확장 정보의 조회에 대한 요청에 대해서 응답을 제공하는 XCMS에 해당된다. 또한 Client는 인증서확장 정보의 조회를 요청하는 XCAS에 해당된다.



(그림 7) SOAP Message 수행과정

(4) XCAS(XML Certificate based Authority Server)

유·무선 단말기 사용자가 로컬 서버에 접속할 경우 사용자의 인증서 패스워드와 인증서확장 정보를획득하여 1, 2차 인증서 인증을 수행하여 로컬 서버의 로그인 여부를 결정하는 서버이다. 본 논문에서 이를 XCAS라 명명한다.

- 인증서 조회
  CA를 통해서 사용자의 인증서 패스워드를 1차 인증한다.
- 인증서확장 정보 조회요청 모듈
  XCMS에 등록된 사용자의 인증서확장 정보를 요청하여, 2차 인증을 위해서 다음과 같이 SOAP 메시지를 작성하여 인증서확장 정보의 조회를 요청한다.

  $XCAS_{res}(CA_{pw}, CA_{cx\_input})$

3.2 XML-Signature 스키마 확장 설계

사용자가 인증서 로그인 화면에서 인증서 패스워드이외에 추가로 입력할인증서확장 정보를 표현하기 위해서 (그림 8)과 같이 XML-Signature 스키마를 확장하여 설계한다.

```
<Signature>
  <KeyInfo>
    <X509Data>
      <X509IssuerName>CN=kimjs, C=KR..</X509IssuerName>
      <X509SerialNumber>1234567</X509SerialNumber>
      <X509SubjectName>Certificate A</X509SubjectName>
      <X509Certificate>MIICSTCCA... </X509Certificate>
      <X509Items> // 확장 부분
        <CertificationCenter> CN_Sign </CertificationCenter>
        <CertificateSerialNumber> CS_0001</CertificateSerialNumber>
        <CertificateDate>2005-06-10 </CertificateDate>
        <CertificatePermitionCode> CN_Sing_Kimjs </CertificatePermitionCode>
        <SignatureAlgorithm> dsa sha1</SignatureAlgorithm>
        <CertificateSubscriber> Kim-js</CertificateSubscriber>
        <PersonalNumber>601011-1234567</PersonalNumber>
      </X509Items>
    </X509Data>
  </KeyInfo>
</Signature>
```

(그림 8) XML-Signature 스키마 확장 설계의 예

〈표 2〉 〈X509Items〉 엘리먼트의 내용

엘리먼트	엘리먼트 내용
<CertificationCenter>	인증기관
<CertificateSerialNumber>	인증서 일련번호
<CertificateDate>	인증서 가입 날짜
<CertificatePermitionCode>	허가코드
<SignatureAlgorithm>	전자서명 알고리즘 이름
<CertificateSubscriber>	가입자
<PersonalNumber>	주민등록번호

확장된 <X509Items>엘리먼트를 구성하고 있는 하위 엘리먼트 이름과 각 엘리먼트들이 포함하고 있는 내용은 <표 2>와 같다.

7개의 엘리먼트 내용은 4.1.3에서 기술할 사용자 로그인 화면에서 랜덤하게 표현되어 사용자의 인증서 패스워드 이외에 추가로 입력하기 위한 항목들이다.

3.3 수행 알고리즘

3.3.1 2단계 인증 알고리즘

제안하는 2단계 로컬 서버 인증을 수행하는 알고리즘은 (그림 9)와 같다.

(그림 9)의 알고리즘은 사용자가 로컬 서버에 접속하기 위해서 인증서 패스워드를 입력할 경우 사용자의 인증기관에 의해서 인증서에 대한 유효성을 1차 인증하고, 또한 사용자가 입력한 인증서확장 정보와 XCMS에 등록된 사용자 인증서확장 정보를 비교하여 2차 인증을 수행하여 결과가 만족하면 로컬 서버에 접속을 허용하는 수행과정을 보여준다.

[알고리즘 1] 2단계 서버 로그인 인증 수행 알고리즘

```
입력 : 인증서 패스워드와 인증서확장 정보
출력 : 2단계 인증을 통한 로컬 서버 접속 여부 결정
begin
{                          // 서버 접속자의 인증서 로그인 정보 추출
  User_login(CA_pw, CA_cx_input) // 사용자 인증서 로그인
  Get_User_logInfo=User_login(CA_pw, CA_cx_input)// 사용자 인증서 로그인 정보 획득

  if (Get_User_logInfo) {
     CA_request(Get_User_logInfo)// 인증기관에 인증 요청
     ResultI = CA_response(CA, CA_CRL) // 인증 요청에 대한 응답
     //1차인증 : 사용자 인증서 정보와 인증기관의 인증서 정보 비교
     if(Get_User_logInfo == ResultI) {
        //2차인증: XCAS와 XCMS사이에서 SOAP 메시지를 이용한 인증서확장 정보 인증
        XCAS_res(M)// XCAS의 인증서확장 정보 요청 메시지
        Result2 = XCMS_req_XCAS(M) // XCMS의 인증서확장 정보 요청 응답 메시지
            if(Get_User_logInfo == Result2)
                server_Access_Success()// 로컬 서버 접속 성공
     }
     else
        server_Access_Fail()// 로컬 서버 접속 실패
  }
}
```

(그림 9) 2단계 인증을 통한 서버 접속 수행 알고리즘

3.3.2 인증서확장 정보 등록 및 조회 알고리즘

인증기관에서 인증서확장 정보 등록에 대한 요청에 대해서 응답하는 알고리즘은 (그림 10)과 같다.

[알고리즘 2] 인증서확장 정보 등록 및 조회 알고리즘

입력 : 인증서확장 정보 등록 요청 및 조회 요청 메시지
출력 : 인증서확장 정보 등록 요청 응답 및 조회 응답 메시지
begin
{ // 인증서확장 정보 등록 요청 및 응답
$CA_{res}(M)$ // 인증서확장 정보 등록 요청 메시지
Message_trans($CA_{res}(M)$)// 인증서확장 정보 등록 요청 메시지 전송
$XCMS_{req\_CA}(M)$ // 인증서확장 정보 등록 요청 응답 메시지 전송
Message_trans($XCMS_{req\_CA}(M)$)// 인증서확장 정보 등록 요청 메시지 전송

// 인증서확장 정보 조회 요청 및 응답
$XCAS_{res}(M)$// XCAS의 사용자 인증서확장 정보 요청 메시지
Message_trans($XCAS_{res}(M)$) // XCAS의 사용자 인증서확장 정보 요청 메시지 전송
$XCMS_{req\_XCAS}(M)$// XCMS의 인증서확장 정보 요청 응답 메시지
Message_trans($XCMS_{req\_XCAS}(M)$) // XCMS의 인증서확장 정보 요청 응답 메시지 전송
}

(그림 10) 인증서확장 정보 등록 및 조회 메시지 전송 알고리즘

(그림 10)의 알고리즘은 인증기관에서 사용자의 인증서확장 정보를 XCMS에 등록 요청하고, XCAS에서 인증서확장 정보 요청 메시지에서 대해서 XCMS에서 인증서확장 정보 등록 요청 응답 및 인증서확장 정보 조회 응답 메시지를 전송하는 알고리즘이다.

4. 2단계 서버 로그인 인증 시스템 구현 및 평가

본 장에서는 3장에서 제안한 XML Signature 스키마 확장을 통해서 2단계 로컬 서버 로그인 인증 시스템을 구현하고, 관련 연구와의 비교분석을 통해서 제안한 시스템을 평가한다.

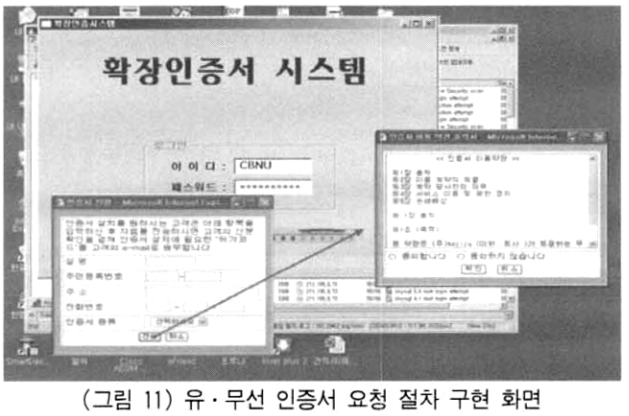
4.1 시스템 구현

본 시스템의 구현환경은 IBM-PC 호환기종으로 Windows XP 운영체제에서 W3C의 SOAP Version 1.2를 사용하였다. 구현은 인증서 요청 및 발급 화면, 2단계 검증을 위한 로그인 화면, 인증서확장 정보를 등록 및 요청하기 위한 SOAP 메시지에 대해서 기술한다.

4.1.1 인증서 요청 및 발급

(1) 유·무선 인증서 요청 SOAP 메시지

사용자와 인증기관 사이에서 인증서를 요청하기 위한 구현 화면은 (그림 11)과 같다.



(그림 11) 유·무선 인증서 요청 절차 구현 화면

인증서를 신청하는 사용자의 인적사항을 입력한 후 인증서 약관에 동의하는 과정에 의해서 인증서 요청이 종료된다. 이 과정에서 사용자가 입력한 인적사항과 재출된 서류에 의해서 사용자의 신분을 확인한후 사용자의 e-mail과 휴대 단말기에 허가코드를 전송한다.

(2) 유·무선 인증서 발급 화면

인증기관에 의해서 사용자의 인증서 발급 요청이 성공적으로 이루어졌을 경우 인증서를 발급하기 위해서 다음과 같은 단계를 수행한다.

- 허가코드 확인과정

사용자의 e-mail과 휴대 단말기에 전송된 허가코드(pc123)를 재확인하기 위해서 (그림 12)와 같은 SOAP 메시지를 작성하여 인증기관에 조회를 요청한다.

사용자의 허가코드 조회 요청에 대한 메시지를 바탕으로 인증기관에서는 (그림 13)과 같이 새롭게 부여된 허가코드를 생성하여 SOAP 메시지로 응답한다.

- 전자서명 생성

인증서에 포함될 전자서명을 생성하기 위해서 서명할 비밀번호를 입력하고, 새롭게 부여 받은 허가코드를 입력한 다음 인증서가 설치될 위치와 인증서의 종류를 선택한다.

- 인증서 설치 및 생성

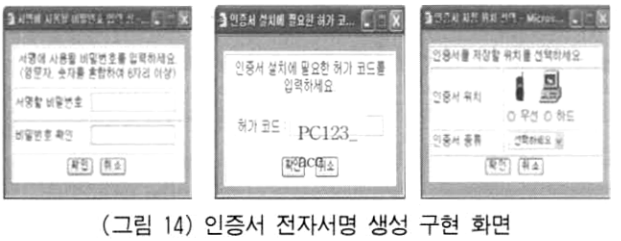
사용자의 전자서명이 생성된 후 인증서가 성공적으로 설치되면 "인증서 보기" 버튼을 클릭하여 인증서를 확인 할 수 있다.

```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Body>
    <SOAPCA:InquiryRequest>
      <a:authentication xmlns:a="http://www.confirm.co.kr">
        <a:PermissionCode> pc123 </a:PermissionCode>
      </a:authentication>
    </SOAPCA:InquiryRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

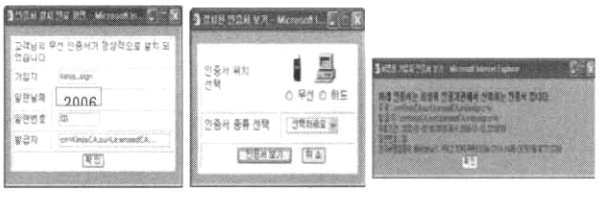
(그림 12) 허가코드 조회 요청 SOAP 메시지

```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Body>
    <SOAPCA:Response>
      <a:authentication xmlns:a="http://www.confirm.co.kr">
        <a:PermissionCode> PC123_acc </a:PermissionCode>
      </a:authentication>
    </SOAPCA:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(그림 13) 허가코드 조회 요청 응답 SOAP 메시지



(그림 14) 인증서 전자서명 생성 구현 화면



(그림 15) 인증서 설치 및 생성 구현 화면

4.1.2 인증서확장 정보 등록 요청 및 응답 SOAP 메시지

(1) 인증서확장 정보 등록 요청 SOAP 메시지

인증기관에서는 사용자의 X509v.3 인증서 정보와 인증서 확장 정보의 파라미터를 XCMS에 등록하기 위해서 (그림 16)과 같은 등록 요청 SOAP 메시지를 전송한다.

```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Body>
    <SOAPXCMS:Register>
      <X509IssuerName> CN=KIM JS</X509IssuerName>
      <X509SerialNumber> 03 </X509SerialNumber>
      <X509SubjectName> Certificate A</X509SubjectName>
      <X509Password>****** </X509Password>
      <X509Certificate>MIIC34PzCCA0+....KTV</X509Certificate>
      <X509CRL> 2010-12-30 </X509CRL>
      <X509Items>
        <CertificateSerialNumber> 03</CertificateSerialNumber>
      </X509Items>
    </SOAPXCMS:Register>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(그림 16) 인증서확장 정보 등록 요청 SOAP 메시지

인증서 등록 요청 메시지는 X509Data 엘리먼트를 구성하고 있는 인증서 발행자, 인증서 키 식별자, 인증서 제목, X509 v3인증서 및 유효기간(CRL)을 포함하고 있으며, 또한 XML-Signature의 확장부분인 <X509Items> 엘리먼트의 내용도 함께 등록 메시지를 작성하여 XCMS에 전송한다.

(2) 인증서확장 정보 등록 요청 응답 SOAP 메시지

로컬 서버에서 사용자의 인증서확장 정보를 등록하기 위한 요청 메시지에 대해 XCMS에서는 (그림 17)과 같은 인증서확장 정보의 등록을 위한 응답 메시를 작성한다.

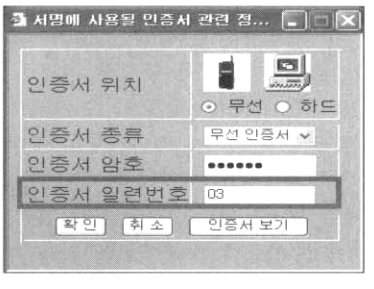
인증기관에서 보낸 인증서확장 정보는 XCMS에서 해당 메소드를 호출하여 X509 v.3 인증서의 확장 정보를 등록하고, 인증서 등록 시리얼 번호와 등록의 성공을 나타내는 메시지를 전송해 준다.

```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Body>
    <SOAPXCMS:RegisterResponse>
      <RegisterSerialNumber>231-645-7754</RegisterSerialNumber>
      <ResultMessage>Certificate verification succeeded!! </ResultMessage>
    </SOAPXCMS:RegisterResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(그림 17) 인증서확장 정보 등록 요청 응답 메시지

4.1.3 2단계 인증 사용자 로그인

XCAS에서는 사용자가 로컬서버에 접속할 경우 (그림 18)과 같은 인증서 패스워드와 인증서확장 정보를 추가로 요구하는 로그인화면을 제공한다.



(그림 18) 2단계 인증을 위한 로그인 화면

불법적인 인증서 도용 및 인증서 패스워드의 해킹으로 문제가 야기될 수 있는 측면을 보완하고자 사용자 로그인 화면의 보안 강화를 위해서 인증서확장 정보에 관련된 <X509Items> 엘리먼트의 내용에서 랜덤으로 하나를 선택한다.

(1) 1단계 인증

1단계 인증은 사용자의 CA_{pw}(인증서 암호)를 가지고 인증기관에 의해서 수행된다.

(2) 2단계 인증

2단계 인증은 인증서확장 정보인 '인증서 일련번호'를 가지고 4.1.4절의 인증서확장 정보 조회 요청 및 응답 SOAP 메시지에 의해서 수행된다.

4.1.4 인증서확장 정보 조회 요청 및 응답 SOAP 메시지

(1) 인증서확장 정보 조회 요청 SOAP 메시지

XCMS에 등록된 사용자의 인증서확장 정보를 조회하기 위해서 사용자가 입력한 인증서 패스워드와 추가로 입력한 인증서확장 정보를 기초로 인증서확장 정보를 조회하기 위한 요청 메시지를 (그림 19)와 같이 작성하여 XCMS에 전송한다.

<X509Password> 엘리먼트는 인증서 패스워드를 포함하고 있으며 <X509Item>은 인증서확장 정보에 대해서 추가로 입력받은 정보(인증서 시리얼 번호)를 포함한다.

XCMS에서는 위와 같은 요청메시지를 수신 받아 인증서확장 정보를 인증하여 로컬 서버 접속의 유무를 결정하기 위한 응답 메시지(그림 18)를 XCAS에 전송 한다.

```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Body>
    <SOAPXCMS:InquiryRequest>
      <X509Password> ****** </X509Password>
      <X509Item>Certificate SerialNumber</X509Item>
    </SOAPXCMS:InquiryRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(그림 19) 인증서확장 정보 조회 요청 메시지

(2) 인증서확장 정보 요청 응답 SOAP 메시지

XCAS에서 인증서확장 정보의 요청에 대한 메시지에 대해서 XCMS에서는 인증서, 인증서 유효기간 그리고 인증서 확장 정보에 대한 내용을 포함하고 있는 인증서확장 정보 요청 응답 메시지를 (그림 20)과 같이 작성하여 응답한다.

조회 결과는 사용자의 인증서 정보를 포함하고 있는 <X509Certificate> 엘리먼트와 인증서 상태 정보를 포함하고 있는 <X509CRL> 엘리먼트 그리고 인증서확장 정보를 포함하고 있는 <X509Items> 엘리먼트로 구성된다. 따라서 사용자가 인증서 패스워드 이외에 추가로 입력한 인증서확장 정보와 (그림 20)의 인증서확장 정보 요청 응답 메시지에 의해서 획득한 인증서 일련번호의 값을 비교하여 로컬 서버의 접속 여부를 결정한다.

```
<SOAP-ENV:Envelope>
  <SOAP-ENV:Body>
    <SOAPXCMS:InquiryResponse>
      <X509Certificate> MIIC34PzCCA0+....KTV</X509Certificate>
      <X509CRL>2010-12-30</X509CRL>
      <X509Items>
        <CertificateSerialNumber>03 </CertificateSerialNumber>
      </X509Items>
    </SOAPXCMS:InquiryResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(그림 20) 인증서확장 정보 요청 응답 메시지

4.2 비교 분석 및 실험평가

본 절에서는 XML-Signature와 로컬 서버 보안에 관련된 연구들과 본 논문에서 제안한 서버 보안기법의 특징을 비교 분석한다. 비교 분석의 대상은 2장의 관련연구에서 기술한 서버 보안에 관한 연구들이다. 또한 XCAS와 XCMS의 두 서버 사이에서 SOAP 메시지에 대한 요청 및 응답에 대한 실험평가를 통해 서버 간의 연산속도를 알아본다.

4.2.1 비교 분석

비교 분석 방법은 기존 보안 관련 연구와 제안한 보안 기법을 중심으로 기능성과 신뢰성 측면에서 비교 분석 및 평가를 수행한다. <표 3>은 비교 평가한 결과이다.

<표 3>은 기능성 측면과 신뢰성 측면으로 구분하여 기존 연구들에서 제안한 XML 기반의 보안 기법과 본 논문에서 제안한 기법을 비교 분석하였다. 먼저 기능성에 관한 호환성과 확장성 측면에서 비교분석하면 [2]는 자신의 고유 식별정보와 기본적으로j 제공되는 보안코드를 결합하여 개인키를 생성하기 때문에 비교적 호환성과 확장성은 제한되어 있지만 2단계 보안기법을 적용하기 때문에 인증서 도용 및 해킹에 대한 안정성이 높다. 또한, 본 논문에서 제안한 기법과 신뢰성분석을 4.2.2절에서 수행한 결과 연산속도가 로그인 횟수에 관계없이 향상된 것을 시뮬레이션을 통해서 검증하였으며, 본 연구에서 제안한 방식은 2단계 검증절차를 거치기 때문에 기존 방법과 비교해서 안정성이 높다고 볼 수 있다. [7]은 일반적인 해시 함수를 사용하기 때문에 비교적 호

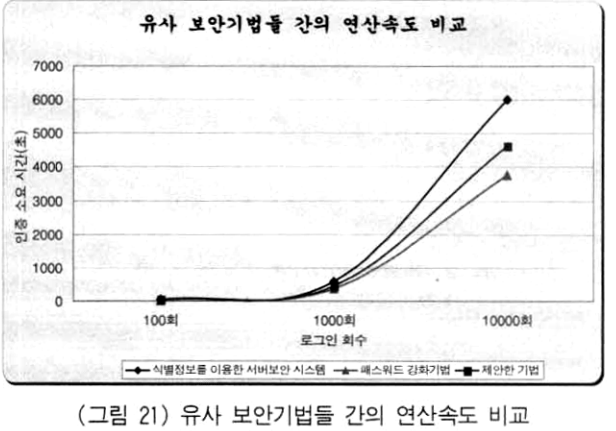
〈표 3〉 유사 보안기법들 간의 비교 분석

보안 기법 / 비교 대상		식별정보를 이용한 서버보안 시스템 [2]	패스워드 강화기법[7]	제안한 기법
기능성	호환성	자신의 고유 식별정보를 이용하여 개인키를 생성하므로 비교적 호환성이 낮음	사용자의 패스워드를 해시 값으로 사용하여 인증하기 때문에 보안성 및 호환성이 높음	XML 기반 서버 보안 및 SOAP 메시지를 기반으로 다양한 시스템 적용에 따른 호환성이 높음
	확장성	키 분산기법이 적용되는 보안 모델에 확장이 용이함	다중 로빙 서버의 패스워드 기반 로그인 시스템에 적용이 용이함	개인/조직의 서버 보안 및 웹 서비스와 같은 전자상거래 분야에 적용이 가능함
신뢰성	연산속도	사용자에게 공개되어 있는 식별정보에 보안코드를 결합하여 인증을 수행하기 때문에 비교적 연산속도가 지연됨	사용자의 패스워드에 해시 값을 적용하여 인증을 수행하기 때문에 연산속도가 빠름	인증서 패스워드와 인증서 확장정보로 2단계 인증을 수행하기 때문에 비교적 연산속도가 지연됨
	검증단계	2단계	1단계	2단계
	안전성	인증서 도용 및 해킹에 대한 대안이 높음	인증서 도용 및 해킹에 대한 대안이 낮음	인증서 도용 및 해킹에 대한 대비책으로 인증서확장 정보를 이용하여 2단계 인증으로 안전성 높음

환성이 높고 확장성이 용이하지만 인증서 도용 및 해킹에 대한 대안이 비교적 적다. 끝으로 본 논문에 제안 기법은 XML-Signature 스키마 확장과 SOAP메시지를 기반으로 하였기 때문에 다양한 시스템에 적용이 가능하여 비교적 호환성과 확장성이 높다. 또한 제안한 기법이 다른 기법에 비해서 인증서의 도용 및 해킹에 대해서 얼마나 안전한가를 보여주는 안전성의 측면에 대한 비교 분석은 기존의 시스템에 비해서 비교적 연산속도는 중간 수준이지만, 인증서 도용 및 해킹에 대한 대비책이 비교적 뛰어나 안전성이 높은 것으로 분석된다.

4.2.2 연산속도 비교

연산속도의 비교는 <표 3>의 유사 보안기법들 간의 연구에서 개인키를 생성하여 인증을 수행하는데 소요되는 연산속도를 사용자의 로그인 수에 따라서 정량적으로 비교분석하면 다음과 같다.

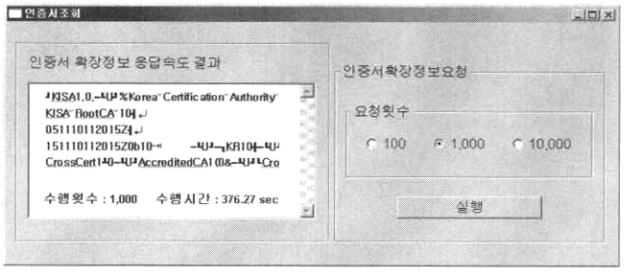


(그림 21) 유사 보안기법들 간의 연산속도 비교

4.2.3 실험평가

XCAS에 등록된 인증서 확장정보를 대상으로 XCMS에서 SOAP 메시지를 1000회 요청한 경우 응답에 대한 수행시간을 다음과 같이 얻을 수 있다. 실험에 사용된 인증서 확장정보는 본 논문에서 제안한 인증서 일련번호, 인증기관명, 인증서 가입 날짜, 허가코드, 전자서명 알고리즘명, 가입자, 주민등록번호의 7개 인증서 확장정보를 대상으로 랜덤하게 발생시켜 실행한 결과이다.

따라서 1000회 수행한 결과 수행시간은 376.27초가 발생되었기 때문에 1회 사용자의 인증서 확장 정보에 대한 요청 및 응답 시간은 평균 0.376초가 소요된다.



(그림 22) 인증서 확장정보 요청에 대한 응답속도 결과

4.2.3 기대효과 및 의의

XML-Signature와 로컬 서버 보안에 관련된 기존 연구들과 제안한 기법을 비교 분석한 결과 다음과 같은 이점으로 기술되어진다.

본 논문에서는 인증서의 도용 및 불법적인 인증서 패스워드 해킹에 대한 보안 메커니즘과 SOAP 메시지를 이용해서 어떠한 환경에서도 정보교환이 가능하도록 호환성과 다양성을 지원하는 메커니즘을 제안하였다.

첫째, 인증서의 도용 및 불법적인 인증서 패스워드 해킹에 대한 대비책으로 서버의 콘텐츠 보호가 가능한 보안 모델을 제시한다.

둘째, SOAP 메시지를 이용해서 어떠한 환경에서도 정보교환이 가능하도록 호환성과 다양성을 지원하는 메커니즘을 제공한다.

셋째, 개인 및 단체에서 서버 보안 정책을 수립하는데 기본적인 시스템 설계 및 구현 방안을 제공한다.

5. 결론 및 향후 연구과제

인터넷이 대중화된 이래 보안에 관한 관심은 개인은 물론 기업이나 국가적인 차원에서 중요하게 다루어져왔다. 특히 개인 정보보호 측면에서 볼 때 무차별한 개인 프라이버시 도용과 정보 자원에 대한 침해 및 파괴로 인하여 그 피해는 개인적인 차원을 떠나 기업이나 국가에 큰 악 영향을 미친다. 따라서 본 연구에서는 개인 및 기업에서 보유하고 있는 서버에 대한 보안 정책으로 기존의 공개키 기반구조와 XML 보안 기술을 적용하고, 인증서의 원격 호출이라는 메커니즘을 제안하여 인증된 사용자만이 서버에 접속을 허용하는 서버 보안 모델을 제시하였다. 또한 공인인증서 사용에 있어서 기존의 인증서 패스워드에만 의존하여 사용자가 로그인하는 일반적인 인증서 로그인 화면에서 인증서확장정보를 추가로 선택하게 하여 보안이 강화된 로그인 화면을 구현하였다.

본 논문의 의의는 인증서의 도용 및 불법적인 인증서 패스워드 해킹에 대한 보안 메커니즘과 SOAP 메시지를 이용해서 어떠한 환경에서도 정보교환이 가능하도록 호환성과 다양성을 지원하는 메커니즘을 제안하였다.

향후 연구 과제는 2단계 인증을 통한 서버의 접속으로 인하여 시스템의 속도가 저하될 수 있는 쟁점에서 인증절차 및 메시지 전송 과정을 고속 처리할 수 있는 메커니즘에 대해서 연구되어야 할 것이다. 또한 공인 인증기관에서 발급한 인증서를 인증서 관리 서버에 등록하고 조회하는 표준화된 프로토콜이 요구되어지며, 메시지를 전달하는 SOAP Message 자체에 대한 완벽한 암호화 알고리즘을 적용하여 네트워크상에서의 메시지 위·변조에 대한 보호기술과 모바일 매체를 통한 로컬 서버 접근 시 무선 인증서에 대한 XML 보안 기술 스펙에 대한 연구가 진일보 되어지는 환경이 요구되어진다.

참 고 문 헌

[1] 김영달, "대칭키 전자서명을 위한 Kailar 책임 로직의 확장 및 전자지불 프로토콜의 책임분석", 한국정보처리학회논문지, 제11권 6호, pp.3046-3059, 1999.

[2] 김영수, "식별정보를 이용한 보안 서버 시스템의 전자서명 모델 및 응용", 한국정보처리학회 논문지 C, 제12-C권 2호, pp.0169-0174 2005.

[3] 문태수, "XML 기반의 안전한 E-Procurement 시스템 설계 및 구현", 한국정보처리학회 논문지 D, 제9-D권 6호, pp. 1043-1054 2002.

[4] 유두규, "NEIS를 위한 PMI 기반의 RBAC 인증과 DB 보완 구현", 한국정보처리학회 논문지 C, 제11-C권 7호, pp. 0981-0992 2004.

[5] 장창복, "무선 환경에서 XML전자서명을 이용한 Java Card 기반 시스템", 한국정보처리학회 논문지 C, 제12-C권 1호, pp.0037-0044 2005.

[6] 정용득, "공개키기반 사용자인증과 암호화를 적용한 영상회의 시스템 설계 및 구현", 한국정보처리학회 논문지 C, 제11-C권 7호, pp.0971-0980 2004.

[7] 정현철, "새로운 패스워드 강화 기법을 이용한 키 로밍 프로토콜", 한국정보처리학회 논문지, 제30권 3호, pp. 0387-0396 2003.

[8] 한명진, "XML 문서 보안을 위한 새로운 XML- Signcryption scheme 설계 및 구현", 한국정보처리학회 논문지 제10-C권 4호, pp.0405-0412 2003.

[9] Andrew Blyth, Daniel Cunliffe and Iain Sutherland, "Security Analysis of XML Usage and XML Parsing," Computers & Security, Vol.22, Issue 6, pp.494-505, September, 2003.

[10] Antonio F. Gmez, Gregorio Martnez and scar Cnovas, "New Security Services based on PKI," Future Generation Computer Systems, Vol.19, Issue 2, pp. 251-262, February, 2003.

[11] Berin Lautenbach, "Introduction to XML Encryption and XML Signature," Information Security Technical Report, Vol.9, Issue 3, pp.6-18, July-September, 2004.

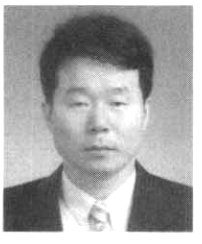
[12] Elisa Bertino, Barbara Carminati and Elena Ferrari, "XML security," Information Security Technical Report, Vol.6, Issue 2, pp. 44-58, June, 2001.

[13] K. Komathy, V. Ramachandran and P. Vivekanandan, "Security for XML Messaging Services a Component-based Approach," Journal of Network and Computer Applications, Vol.26, Issue 2, pp.197-211, April, 2003.

[14] OASIS, http://xml.coverpages.org/WSS-Core-01-20020920.pdf, 2002.

[15] Stephen Farrell and Michael Zolotarev, "XML and PKIWhat's the Story," Network Security, Vol.2001, Issue 9, pp.7-10, September, 2001.

[16] W3C, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212, 2002.



김 용 화

e-mail : kyh@chonbuk..ac.kr

1985년 전북대학교 전산통계학과(학사)

1991년 전북대학교 대학원 전산통계학과 (석사)

2000년~현재 전북대학교 대학원 전산통계학과 박사과정

관심분야 : XML, 객체지향, 성능평가

김 진 성

e-mail : kpjiju@chonbuk.ac.kr

1992년 원광대학교 신문방송학과 (사회과학사)

2002년 전북대학교 대학원 컴퓨터 정보학과(석사)

2006년 전북대학교 대학원 컴퓨터 통계정보학과(박사)

관심분야 : XML, 객체지향 모델링, 워크플로우(XPDL), W3C 웹 서비스, PKI 등

김 용 성

e-mail : yskim@chonbuk.ac.kr

1978년 고려대학교 수학과(학사)

1984년 광운대학교 대학원 전산학과(석사)

1992년 광운대학교 대학원 전산학과(박사)

1985년~현재 전북대학교 전자정보공학부 교수

1996년~1998년 한국학술진흥재단 전문위원

관심분야 : XML, 사용자중심의 정보검색, 다중 사용자 인터페이스, W3C 웹 서비스 등