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

Design and Implementation of Two-phase server Certification system based on XML-Signature

김용화[1]

Yong Hwa Kim[1]

요약

본 논문은 다양한 웹 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 구현하여 검증한다. 제안할 인증 시스템은 XML 기반의 인증서를 온라인상에서 요청 및 발행하고 인증기관에서 제공한 인증서확장 정보를 인증서 관리 서버에 등록 한 후 사용자의 인증서 패스워드로 인증기관에 의해서 1차 인증을 수행하도록 한 후 인증서 패스워드 이외에 추가로 입력한 인증서확장 정보와 인증서 관리서버에 등록된 사용자의 인증서확장 정보를 SOAP 메시지로 요청한 후 두값을 비교하여 2차 인증을 수행하는 보안이 강화된 인증 시스템을 제안하는데 목적이 있다.
본 논문의 의의는 인증서의 도용 및 불법적인 인증서 패스워드 해킹에 대한 보안 메커니즘과 SOAP메시지를 이용해서 어떠한 환경에서도 인증을 기반으로 정보교환이 가능하도록 호환성과 다양성을 지원하는 메커니즘을 제안하는데 있다.

핵심어: 서버보안, XML-인증, SOAP, 보안검증, PKI, 인증시스템

Abstract

This paper proposes a two-phase server certification system through XML-Signature schema extension to protect the server's information resources which offer various web contents. This system design and implementation. Certification system to propose certificate of XML base in on-line request and publish. After we register certificate extension information that offer in CA (Certification Authority) to (XCMS) certificate management server certificate password to base by CA the first certification achieve. Also, it is new Authentication System who will request the certificate extension information that the user inputs in addition, except certificate password and certificate extension information that is registered to XCMS and run the second authentication achieve.

Keyword: Server Security, XML-Signatrue, SOAP, X509 v.3 Certificate, PKI

1 Department of Computer Center, Cheonbuk Natational Univ, Bakjae-Ro, DuckJin-Gu, JeonJu-City, Cheonbuk-Do 54896, Korea e-mail: yhkim@jbnu.ac.kr
Received(May 31.2015), Review (June 12.2015), Accepted(June 30.2015)

1. 서론

오늘날 무선 인터넷에 관련된 기술의 향상과 해킹 기술의 발전으로 인하여 개인 및 시업 그리고 국가에 대한 정보 자산이 손쉽게 유출되고 파괴되는 경우가 빈번하게 발생되고 있다. 또한 여기에 대한 보안기술과 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].

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 시스템 이다. 이를 위해 인증기관에서 발행된 인증서 확장 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 위한 OCSP(Online Certificate Status Protocol)의 문제 해결 방안으로 SOAP 메시지를 사용하여 플랫폼에 독립적으로 서버 접속을 허용하도록 하였다[8-10]. 따라서 본 논문에서는 XML Signature 스키마를 확장하여 2단계 서버 로그인 인증 시스템을 설계 및 구축하여 XML특성을 활용한 시스템간의 원할 한 상호연동과 인증서 패스워드 이외에 추가로 인증서확장 정보를 입력하게 하여 기존의 인증서 패스워드만의 입력방식에 대해서 더 한층 안전성을 보장하는 서버 보안 모델을 제안하는데 목적이 있다.

본 논문의 구성은 제 2장에서는 관련연구로서 XML 기반의 보안기술에 관한 기존 연구와의 비교분석 및 XML Signature의 스키마 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. 관련 연구

2.1 XML 기반 보안 기법

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 관련연구들을 분석한다.

먼저 서버 보안에 관한 연구들은 [2]와 [3]이 있다. [2]는 식별정보를 이용하여 서버공격으로부터 야기되는 위협을 감소시키는 서명 시스템을 제안 하였고, [3]은 패스워드 기반 로밍 시스템에서 사용자의 해시 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. [3]은 패스워드 강화기법으로 해시 값을 적용하기 때문에 전자상거래 및 서버 보안 분야에 포괄적으로 적용이 가능하지만 기존에 제안한 XML 기반 보안 기법과 큰 차이가 없을 수 있다. 따라서 본 논문에서는 이러한 분석결과를 토대로 호환성 및 안전성을 고려한 새로운 인증서 로그인 강화기법을 제안한다. 또한 XML 전자서명 기법에 관한 연구에는 [1][4][5]이 있다. [1]은 전자상거래를 위한 비대칭 키 전자서명 기법으로 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 구성요소를 변경 및 추가하여 확장하였다 참고문헌[8]은 이기종간의 시스템에서 동작 가능하고 XML 문서를 보호할 수 있는 보안 메커니즘으로 XML-Signature을 설계하고 구현하였다. 즉, 웹 서비스 보안에 관한 연구를 기반으로 서비스 호출을 담당하는 SOAP 메시지에 XML-Signature을 적용하여 보안 서비스를 제공하는 기법을 제안하였다 [4].

참고문헌[5]은 XML-Signature**와** XML-Encryption에 대한 스키마 예문과 하위 엘리먼트에 대해서 상세하게 기술하고 있다. 이와 같은 XML 전자서명 기법에 관한 연구 중에서 특히 [4]과 [5]에서 제안한 XML-Signature와 SOAP 메시지에 대한 활용 기법은 본 논문에서 응용 및 활용하였다.

2.2 XML-Signature

XML-Signature[6]는 사이버 상에서 거래를 증명하거나 신우너확인이 필요할 때 이를 확실히 증명해주는 증명 수단으로 사용된다.

다음 [그림 2-1]은 W3C 권고안에서 발표한 XML-Signature 엘리먼트[6][7]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 2-1] XML-Signature Element 구성요소

[Fig. 2-1] Compont of XML-Signature Element

<SignedInfo> 엘리먼트는 서명정보가 규격화되는 알고리즘을 명시한 <CanonicalizationMethod> 엘리먼트와 서명을 위한 알고리즘을 명시하고 있는 <SignatureMethod> 엘리먼트 그리고 서명 데이터를 압축하고 압축한 결과를 포함하고 있는 <Reference> 엘리먼트로 구성된다. 또한 <SignatureValue> 엘리먼트는 <SignedInfo> 엘리먼트에서 계산된 서명을 포함하고 있다[8].

<SignatureValue>dp 기록된 서명(Signatrue)을 사용하기 위해 키 정보를 제공하는 엘리먼트로 KeyName, KeyValue, X509Data 엘리먼트로 구성되어 있다. <KeyName> 엘리먼트는 전자서명이

나 암호화를 수행하는 사람이 수신자에게 공개 키를 식별하기 위해 사용되는 문자열을 포함하며, <KeyValue> 엘리먼트는 전자서명을 확인하고 데이터를 복화화하며 키를 일치시키는데 필요한 공개 키의 실제 값을 포함하고 있는 엘리먼트 이다. 또한 <X509Data> 엘리먼트는 X509인증서에 관한 정보를 포함하고 있다.

2.3 SOAP(Simple Access Object Protocol)

SOAP는 분산 환경에서 정보교환을 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[9][10].

(1) 원격 메소드 요청 SOAP Message

원격 서버의 해당 메소드를 호출하여 데이터를 처리하기 위한 원격 메소드 요청 SOAP Message는 HTTP Body를 통해 SOAP 메시지가 전달된다. 따라서 요청 SOAP메시지는 HTTP Header 부분과 SOAP Envelope 부분 그리고 실제 메시지를 포함하고 있는 SOAP BODY 부분으로 구성된다. 원격 메소드 요청 SOAP 메시지에 대한 예는 다음 [그림 2-2]와 같다.

```
<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 2-2] 원격 메소드 SOAP 메시지 예
[Fig. 2-2] Example Soap massage of Renote method

SOAP Body 부분에서는 XML 형식의 교환 정보를 기술하는 부분으로 http://www.confirm.co.kr URL로 신원 확인을 요청하기 위해 사용자의 ID와 Password를 포함하고 있는 SOAP메시지이다.

(2) 원격 메소드 응답 SOAP메시지

원격 서버의 XML형식의 교환 정보가 전송되어 해당 메소드에 의해 처리된 결과를 요청한 사용자에게 응답하기 위한 원격 메소드 응답 SOAP 메시지를 의미 한다.

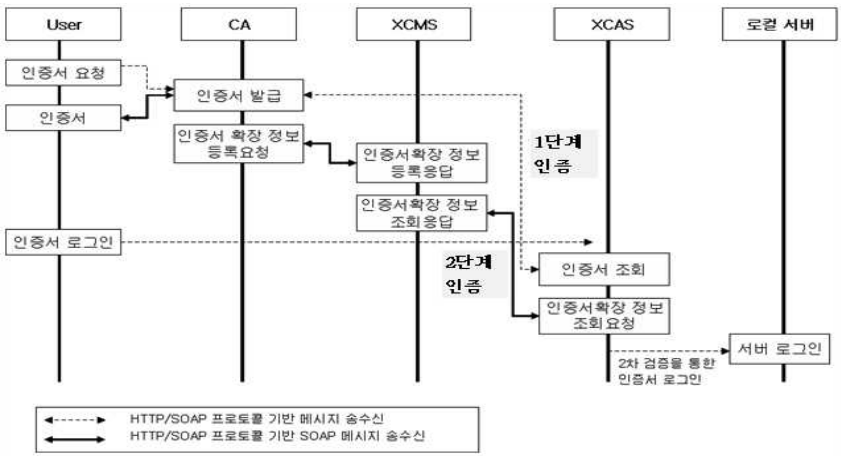
3. 2단계 서버 로그인 인증 시스템 설계

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 인증서 확장 정보를 인증서 관리 서버에 등록하여 인증서 패스워드로 1차 인증하고, SOAP 메시지를 통해서 인증서 확장 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 시스템 구성도

본 논문에서 제안하는 XML-Signature 스키마 확장을 통한 2단계 인증을 위한 서버 로그인 시스템의 전체 구성도는 다음 [그림 3-1]과 같다.



[그림 3-1] 시스템 구성도

[Fig. 3-1] System structure

3.2 XML-Signature 스키마 확장 설계

사용자가 인증서 로그인 화면에서 인증서 패스워드 이외에 추가로 입력할 인증서 확장 정보를 표현하기 위해서 다음 [그림 3-2]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 3-2] XML-Signature 스키마 확장

[Fig. 3-2] Extended XML-Signature Schema

3.3 수행 알고리즘

제안하는 2단계 로컬 서버 인증을 수행하는 알고리즘은 다음 [그림 3-3]와 같다.

ISSN: 2508—9099 JDAEM

[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_ex_input) // 사용자 인증서 로그인
  Get_User_logInfo=User_login(CA_pw, CA_ex_input)// 사용자 인증서 로그인 정보 획득

  if (Get_User_logInfo) {
     CA_request(Get_User_logInfo)// 인증기관에 인증 요청
     Result1 = CA_response(CA, CA_CRL) // 인증 요청에 대한 응답
     //1차인증 : 사용자 인증서 정보와 인증기관의 인증서 정보 비교
     if(Get_User_logInfo == Result1) {
        //2차인증: XCAS와 XCMS사이에서 SOAP 메시지를 이용한 인증서확장 정보 인증
        XCAS_req(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 3-3] 2단계 인증을 통한 서버 접속 수행 알고리즘

[Fig. 3-3] Server connection algorithm through Two-phase certification

[그림 3-3]의 알고리즘은 사용자가 로컬 서버에 접속하기 위해서 인증서 패스워드를 입력할 경우 사용자의 인증기관에 의해서 인증서에 대한 유효성을 1차 인증하고, 또한 사용자가 입력한 인증서 확장 정보와 XCMS에 등록된 사용자 인증서 확장 정보를 비교하여 2차 인증을 수행하여 결과가 만족하면 로컬 서버에 접속을 허용하는 수행 과정을 보여준다.

인증기관에서 인증서확장 정보 등록에 대한 요청에 대해서 응답하는 알고리즘은 다음 [그림 3-4]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
$CA_{rrs}(M)$ // 인증서확장 정보 등록 요청 메시지
Message_trans($CA_{rrs}(M)$)// 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
$XCAS_{rrs}(M)$// XCAS의 사용자 인증서확장 정보 요청 메시지
Message_trans($XCAS_{rrs}(M)$) // 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 3-4] 인증서 확장 정보등록 및 조회 메시지 전송 알고리즘
[Fig. 3-4] Catalog of Extended certification information and algorithm of reference message transmissin

[그림 3-4]의 알고리즘은 인증기관에서 사용자의 인증서 확장 정보를 XCMS에 등록 요청하고, XCAS에서 인증서 확장 정보 요청 메시지에 대해서 XCMS에서 인증서 확장 정보 등록 요청 응답 및 인증서 확장 정보 조회 응답 메시지를 전송하는 알고리즘이다.

4. 2단계 서버 로그인 인증 시스템 구현 및 평가

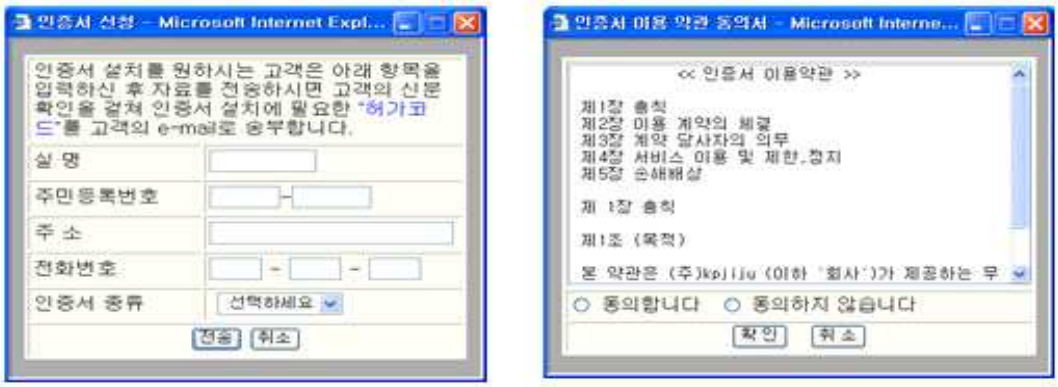
본 장에서는 3장에서 제안한 XML-Signature 스키마 확장을 통해서 2단계 로컬 서버 로그인 인증시스템을 구현하고, 관련 연구와의 비교분석을 통해서 제안한 시스템을 평가한다.

4.1 시스템 구현

본 시스템의 구현환경은 IBM-PC 호환기종으로 Window XP 운영체제에서 W3C의 SOAP Version1.2를 사용하였다. 구현은 인증서 요청 및 발급 화면, 2단계 검증을 위한 로그인 화면, 인증서확장 정보를 등록 및 요청하기 위한 SOAP 메시지에 대해서 기술한다.

(1) 유.무선 인증서 요청 SOAP 메시지

사용자와 인증기관 사이에서 인증서를 요청하기 위한 구현 화면은 다음 [그림 4-1]과 같다.



[그림 4-1] 인증서 확장 정보 및 조회 메시지

[Fig. 4-1] Extended certification information and reference message

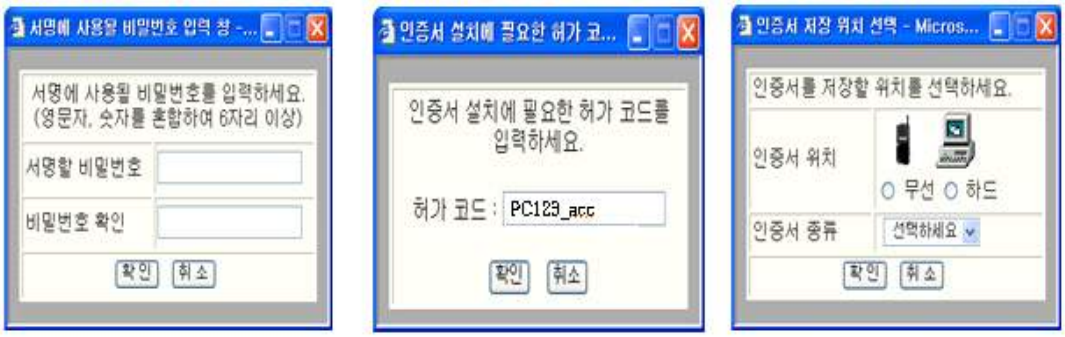
인증서를 신청하는 사용자의 인적사항을 입력한 후 인증서 약관에 동의하는 과정에 의해서 인증서 요청이 종료된다. 이 과정에서 사용자가 입력한 인적사항과 제출된 서류에 의해서 사용자의 신분을 확인한 후 사용자의 e-mail과 휴대 단말기에 허가코드를 전송한다.

(2) 유무선 인증서 발급 화면

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

● 전자서명 생성

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



[그림 4-2] 전자서명 생성 구현 화면

[Fig. 4-2] Implementation Screen of digital Signature

● 인증서 설치 및 생성

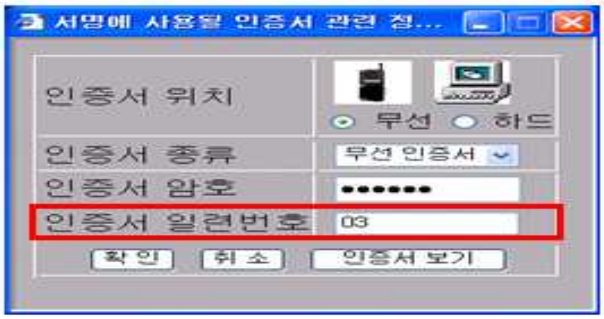
사용자의 전자서명이 생성된 후 인증서가 성공적으로 설치되면 "인증서 보기" 버튼을 클릭하여 인증서를 확인 할 수 있다.

[그림 4-3] 인증서 설치 및 구현 화면

[Fig. 4-3] Screen of certification Installation and Implementation

(3) 2단계 인증 사용자 로그인

XCAS에서는 사용자가 로컬 서버에 접속할 경우 다음 [그림 4-4]과 같은 인증서 패스워드와 인증서확장정보를 추가로 요구하는 로그인 화면을 제공한다.



[그림 4-4] 2단계 인증을 위한 로그인 화면
[Fig. 4-4] Log-in Screen for two-phase certification

불법적인 인증서 도용 및 인증서 패스워드의 해킹으로 문제가 야기될 수 있는 측면을 보완하고자 사용자 로그인 화면의 보안 강화를 위해서 인증서확장 정보에 관련된 <X509Item> 엘리먼트의 내용에서 랜덤으로 하나를 선택한다.

● 1단계 인증

1단계 인증은 사용자의 CApw(인증서 암호)를 가지고 인증기관에 의해서 수행된다.

● 2단계 인증

2단계 인증은 인증서 확장정보인 '인증서 일련번호'를 가지고 인증서 확장 정보 조회 요청 및 응답 SOAP메시지에 의해서 수행된다.

4.2 비교 분석 및 평가

본 절에서는 XML-Signature와 로컬 서버 보안에 관련된 연구들과 본 논문에서 제안한 서버 보안 기법의 특징을 비교 분석한다. 비교 분석의 대상은 2장의 관련 연구에서 기술한 서버 보안에 관한 연구 들인다.

4.2.1 비교 분석 및 평가

비교 분석 및 평가 방법은 기존 보안 관련 연구와 제안한 보안 기법을 중심으로 기능성과 신뢰성 측면에서 비교 분석 및 평가를 수행한다. 다음 [표 4-1]은 비교 평가한 결과이다.

[표 4-1] 비교 평가

[Table 4-1] Compersion of 3method

비교대상 \ 보안 기법		식별정보를 이용한 서버 보안 시스템 [2]	패스워드 강화 기법 [7]	제안한 기법
기능성	호환성	자신의 고유 식별정보를 이용하여 개인키를 생성하므로 비교적 호환성이 낮음	사용자의 패스워드를 해시 값으로 사용하여 인증하기 때문에 보안성은 높지만 비교적 호환성이 높음	XML 기반 서버 보안 및 SOAP 메시지를 기반으로 다양한 시스템 적용에 따른 호환성이 높음
	확장성	키 분산 기법이 적용되는 보안 모델에 확장이 용이함	다중 로밍 서버의 패스워드 기반 로그인 시스템에 적용이 용이함	개인/조직의 서버 보안 및 웹 서비스와 같은 전자상거래 분야에 적용이 가능함
신뢰성	연산속도	중간	빠름	중간
	검증단계	2단계	1단계	2단계
	안전성	인증서 도용 및 해킹에 대한 대안이 비교적 높음	인증서 도용 및 해킹에 대한 대안이 비교적 낮음	인증서 도용 및 해킹에 대한 대비책으로 인증서 확장 정보를 이용하여 2단계 인증으로 안전성 높음

[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 [1]은 자신의 고유 식별정보와 기본적으로 제공되는 보안코드를 결합하여 개인키를 생성하기 때문에 비교적 호환성과 확장성은 제한되어 있지만 2단계 보안기법을 적용하기 때문에 인증서 도용 및 해킹에 대한 안전성이 높다. [7]은 일반적이 해시 함수를 사용하기 때문에 비교적 호환성이 높고 확장성이 용이하지만 인증서 도용 및 해킹에 대한 대안이 비교적 적다. 끝으로 본 논문에 제안 기법은 XML-Signature 스키마 확장과 SOAP 메시지를 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 중간수준이지만, 인증서 도용 및 해킹에 대한 대비책이 비교적 뛰어나 안전성이 높은 것으로 분석된다.

5. 결론 및 향후 연구과제

인터넷이 대중화된 이래 보안에 관한 관심은 개인은 물론 기업이나 국가적인 차원에서 중요하게 다루어져 왔다. 특히 개인 정보보호 측면에서 볼 때 무차별한 개인프라이버시 도용과 정보 차원에 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 인증서확장 정보를 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.

References

[1] Y. D. Kim and S. Y. Han, KIPS Journal. (1999), Vol.6, No.11, pp.3046-3059.

[2] Y. S. Kim and S. J. Shin, KIPS Journal (2005), Vol.12, No.2, pp.169-174.

[3] A. Blyth, D. Cunliff, I. Sutherland, Computers & Security. (2003), Vol.22, No.6, pp.494-505.

[4] A. F. Gmez, G. Martnez S. Cnovas, Future Generation Computer Systems. (2003), Vol.19, No.2, pp.251-262.

[5] B. Lautenbach, Information Security Technical Report. (2004), Vol.9, No.3, pp..6-18.

[6] P. H. Baker, C. Kaler, R. Monzillo, A. Nadalin, Advancing open standards for the information society. (2002)

[7] J. W. Lee, The korea Academia-industri cooperation society. (2011).

[8] J. Park, N. Kang, J.KICS. (2013), Vol.38, No.5.

[9] B. Lee, Journal of Security Engineering. (2014), Vol.11, No.4, pp.273-286.

[10] http://www,ietf.org/rfc/rfc2459.txt

ISSN: 2508—9099 JDAEM