PKI와 안전한 연동을 위한 XKMS 개선방안 연구

이상호° 남길현*
국방대학교 전산정보학과
supaf716@chol.com°, khnam@kndu.ac.kr*

A Study on Improvement of XKMS for Secure Interworking with PKI

Sang-Ho Lee°, Kil-Hyun Nam*
Dept. of Computer & Information, Korea National Defense University

요 약

최근 XML을 기반으로 한 웹서비스는 인터넷 전자상거래와 인터넷을 기반으로 한 서비스통합 등 다양한 분야에서 활용되고 있으며 웹서비스를 이용한 메시지 및 문서를 안전하게 송수신 하기위해 XKMS기반 하에 XML전자서명, XML암호화 등이 표준화 되어 있다. 그러나 웹서비스를 위한 XML기반 PKI서비스인 XKMS는 PKI와의 연동방안이 제시되어 있지 않으며 PKI와 XKMS간의 상호인증이 보장되어 있지 않고 서비스거부공격과 재연공격 등에 취약점이 있는 등 여러 가지 취약점이 분석되고 있다. 본 논문에서는 CA발행 공인인증서를 활용한 XKMS와 PKI서버간의 상호인증방안을 제시하고 메시지 송수신 시 nonce값을 이용하여 재연공격을 방지할 수 있는 메시지 형식을 정의함으로써 보다 안전하게 XKMS와 PKI가 연동을 하는데 도움이 되고자 한다.

1. 서 론

최근 웹서비스의 기반언어인 XML(eXtensible Markup Language)이 인터넷 전자상거래와 데이터 전송 및 검색 등에서 광범위하게 이용됨에 따라 XML문서에 대한 보안이 웹서비스 보안문제의 핵심으로 대두되고 있다. 웹서비스 상에서 각종 데이터는 인터넷망에 오픈되어 존재하게 되며, 이러한 웹상에서의 문서처리는 제3자에 의해 위조나 변경이 가능하다. 이에 데이터 및 문서를 보호하는 것은 필수적인 사안이며, XML문서보안에 대한 연구개발 또한 국내외에서 활발히 진행되고 있다.

다양한 웹서비스 보안 주제 중에서 XML문서보안과 관련된 주제로는 XML전자서명[1], XML암호화[2], XKMS[3] 등이 있으며 XML전자서명과 XML암호화는 XKMS를 활용한 안전한 키관리와 키검증이 보장되어야만 적용이 가능한 기술이다. 따라서 XKMS는 XML전자서명과 XML암호화를 하기 위한 필수 기반기술이라 할 수 있다.

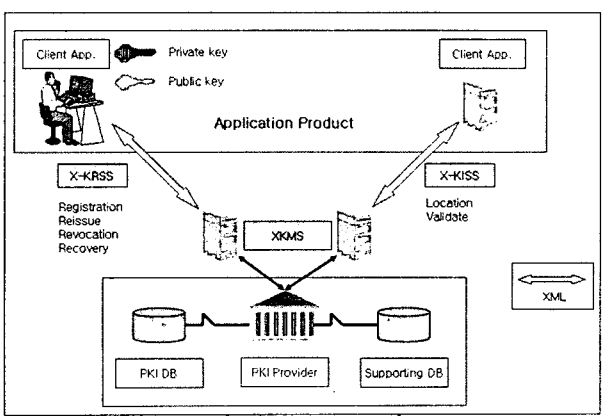
XML기반 차세대 PKI[4]기술인 XKMS는 보안과 관련하여 아직 해결되어야 할 사항들이 많이 있다. 예상되는 보안취약점으로는 재연공격, DoS공격, XKMS와 PKI 서비스 간 상호인증절차 및 메시지 송수신 절차 부재 등이 해결되어야 할 과제들이다.

따라서 본 논문에서는 XKMS와 PKI간 상호인증을 위해 CA발행 공인인증서를 활용하여 PKI와의 메시지 송수신 시 전자서명 검증을 통한 송수신 메시지간의 무결성, 상호인증을 보장하며 메시지 송수신 시 nonce값을 정의하여 재연공격을 방지할 수 있는 방안을 제안한다.

2. 관련연구

2.1 XKMS 개요

XKMS는 웹서비스에서 키의 등록, 키 정보의 해결이나 유효성 검증 등의 서비스 인터페이스와 프로토콜을 정의하고 있으며, XML기반의 공개키 관리를 위한 프로토콜로 공개키의 효율적인 공유기능을 제공한다. XML암호화, XML전자서명 등은 많은 부분에서 PKI에 의존하고 있는데, 기존 PKI를 이용하기 위해서는 복잡한 데이터 구조나 API를 구현해야 한다. 이를 웹서비스를 통해 해결하고 이용 가능하게 하는 것이 XKMS의 목적이다.



[그림 1] XKMS 프로세스

XKMS는 X-KISS와 X-KRSS로 구성되며 X-KISS는 키 정보처리 서비스를 지원하기 위한 프로토콜로 위치서비스

와 검증서비스를 제공하고, X-KRSS는 키 등록을 지원하기 위한 프로토콜로 등록, 복구, 폐기, 재발행 등의 서비스를 제공한다.

XKMS는 웹서비스의 메시지 송수신 표준프로토콜인 XML기반 SOAP메시지 형식으로 클라이언트와 메시지를 송수신 하게되며 PKI와의 메시지 송수신에 관한 형식 및 절차에 관한 사항은 언급되어 있지 않다. XKMS의 전반적은 프로세스는 [그림 1]과 같다[3][5].

2.2 XKMS의 보안 취약점

XKMS는 아직 상용제품으로 실제 구현된 사례는 없으며 연구단계의 시제품 정도의 개발에 머무르고 있다. 이는 XKMS가 아직 미결된 보안상의 취약점을 보유 하고 있기 때문이다.

먼저 생각할 수 있는 취약점은 재연공격이다. 공격자가 XKMS와 클라이언트 혹은 XKMS와 PKI서비스 간 송수신되는 메시지를 절취하여 클라이언트 혹은 XKMS 및 PKI서버에 동일한 메시지를 다시 전송하여 서비스 장애를 유발시킬 수 있을 것이다. 두 번째로 생각할 수 있는 취약점은 DoS공격이다. 클라이언트와 XKMS서버 간 혹은 XKMS서버와 PKI서비스 간 특정 서버에게 다량의 메시지를 집중적으로 전송하여 서비스를 할 수 없게 만드는 서비스 거부공격이 가능하다.

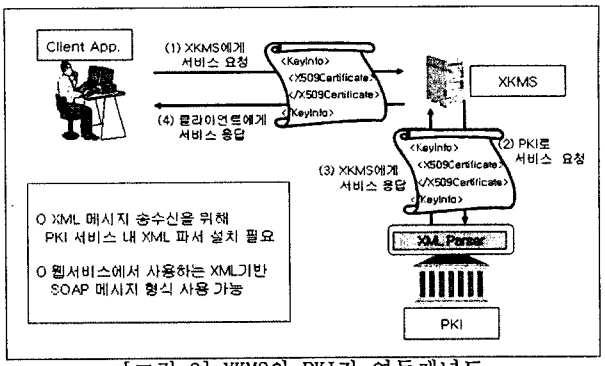
그리고 현재 XKMS 2.0에는 웹서비스의 클라이언트와 XKMS사이의 다양한 서비스에 대한 메시지 송수신 절차 및 형식은 명세가 되어있으나 XKMS와 PKI간의 메시지 송수신 절차 및 형식에 대해서는 전혀 언급이 되어있지 않다. 또한 XKMS서버와 PKI서버 간 상호인증절차가 부재하여 악의를 가진 공격자가 메시지를 전송하더라도 상대가 정당한 XKMS서버 또는 PKI서버인지 판단할 수 없다.

3. PKI와 연동을 위한 XKMS개선방안

3.1 PKI와 연동방안

PKI와의 연동방안은 크게 두 가지로 생각해 볼 수 있다. 첫번째 방안은 XKMS서버에 PKI 모듈 인터페이스를 설치하여 SOAP메시지를 PKI서비스에서 해석 할 수 있는 형식으로 변환하여 전송하도록하는 방안이다. 이 방안은 XKMS 서버마다 PKI 모듈 인터페이스 프로그램을 설치해야 하는 불편함이 있을 수 있다.

두번째 방안은 PKI서비스 내에 XML 파서를 설치하여 기존의 웹서비스 클라이언트와 XKMS간의 전송메시지 형식인 XML기반 SOAP메시지형식을 그대로 재사용하는 방안이다. 이 방안은 우리나라의 경우를 예를 들면 6개 공인인증기관의 서버에 XML파서를 설치하면 되므로 XKMS서버에 별다른 프로그램의 설치 없이 연동이 가능하다. 따라서 본 논문에서는 두번째 방안을 기준으로 SOAP메시지 형식을 재사용한다는 가정하에 개선된 메시지 형식을 제안하고자 한다. [그림 2]는 본 논문에서 제안하는 XKMS와 PKI간의 연동 개념도이다.



[그림 2] XKMS와 PKI간 연동개념도

3.2 개선된 XKMS 명세구조

3.2.1 가정사항

개선된 XKMS명세구조를 정의하기 위해서는 두 가지 가정사항이 필요하다. 첫번째는 PKI서버에 XML파서를 설치해야 한다는 것이다. 제시하는 XKMS 명세구조는 기존 웹서비스를 이용하는 클라이언트와 XKMS간 메시지 송수신 시 활용하는 XML기반 SOAP 메시지 형식을 XKMS와 PKI서버 간에도 그대로 사용한다는 가정 하에 정의된 명세구조이다.

두번째는 XKMS서버의 CA발행 공인인증서 보유이다. CA발행 공인인증서는 XKMS서버와 PKI서버간의 상호인증을 위해 사용된다. XKMS서버는 자신이 정당한 XKMS서버임을 증명하기 위해 자신의 개인키를 이용하여 전자서명을 생성하여 메시지를 전송하며 PKI서버는 XKMS의 공개키를 이용하며 전자서명을 검증함으로써 XKMS서버를 인증하게 된다. 또한, 전자서명을 이용하게 되므로 상호인증은 물론이고 메시지의 무결성도 보장 받을 수 있다.

3.2.2 추가 XML 요소 정의

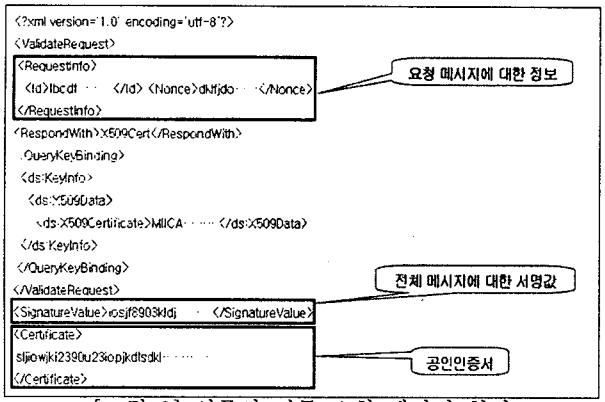
개선된 XKMS명세구조를 정의하기 위해서는 [표 1]과 같이 XML요소 몇 가지를 추가로 정의해야한다.

[표 1] XML 추가요소

요 소 명	내 용
RequestInfo	요청메시지 정보를 포함한 요소로서 하위요소로 <Id>, <Nonce>를 가진다.
Id	요청메시지의 고유한 ID값을 포함
Nonce	메시지 절취를 통한 재연공격을 막기 위한 임의의 값
SignatureValue	전송 메시지의 모든 내용을 전자서명하여 생성된 서명값
Certificate	자신이 보유하고 있는 공인인증서
ReplyInfo	요청메시지에 대한 응답정보를 포함한 요소로서 <Id>, <Nonce>를 하위요소로 가진다.

3.2.3 메시지 형식

추가로 정의한 XML요소를 반영하면 XKMS와 PKI서비스 간 송수신 메시지는 무결성 보장과 함께 재연공격을 방어할 수 있다. 기존의 웹서비스 활용 클라이언트와 XKMS 간의 메시지 형식에 위에서 정의한 새로운 요소 몇 가지만 추가하면 보안이 한층 강화된 메시지 송수신이 가능하다. [그림 3]은 XKMS가 PKI서비스에게 인증서 검증서비스를 요청하는 메시지 형식이다.



[그림 3] 인증서 검증 요청 메시지 형식

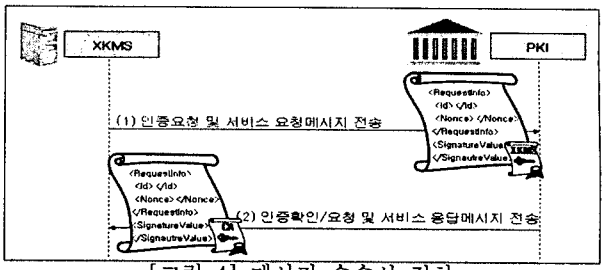
<RequestInfo>요소에 <Id>와 <Nonce>를 포함하여 재연공격을 방지할 수 있으며 <Signature>요소는 요청메시지 전체를 공인인증서에 등록된 공개키와 쌍을 이루는 개인키로 전자서명을 생성하여 PKI서버가 전자서명을 검증할 수 있도록 한다. 위 메시지에 대한 응답메시지는 요청메시지 형식과 유사하다. <RequestInfo>요소대신 <ReplyInfo>요소로 변경하면 된다.

위의 예는 XKMS서비스 중 X-KISS의 검증서비스에 대한 메시지 형식만 나타내었으나 X-KISS의 위치서비스나 X-KRSS의 등록, 복구, 폐기, 재발행 서비스의 송수신 메시지 형식 역시 <RequestInfo>요소와 <ReplyInfo>요소와 <Signature>요소만 추가하면 동일한 효과를 나타낸다.

제안하는 메시지 형식은 PKI와 연동을 위한 XKMS개선 방안이지만 기존의 XKMS와 웹서비스 클라이언트간의 메시지 송수신에서도 클라이언트와 XKMS간 상호인증 부재, 재연공격 가능, 메시지 무결성 보장 등의 유사한 보안 취약점이 있으므로 응용하면 XKMS와 웹서비스 클라이언트 간 메시지 송수신에도 적용할 수 있을 것이다.

3.2.4 메시지 송수신 절차

XKMS와 PKI의 모든 메시지는 요청메시지와 응답메시지로 구성된다. XKMS와 PKI는 모두 CA발행 공인인증서를 보유하고 있으므로 각각의 요청메시지와 응답메시지는 공인인증서를 활용하여 전자서명값 생성이 가능하다. 이 값의 검증을 통해 송수신 메시지의 무결성 보장은 물론 상호인증이 보장된다. [그림 4]는 메시지 송수신 절차에 대한 일반적인 개념도를 나타낸다.



[그림 4] 메시지 송수신 절차

4. 보안성 분석

제안한 XKMS명세는 기존의 XKMS 2.0에 비해 몇 가지 보안취약점이 개선되었다. 첫째, CA에 등록된 공개키와 쌍을 이루는 개인키로 생성한 전자서명을 포함하여 전송된 메시지를 수신측에서 CA발행 공인인증서에 등록된 공개키를 활용하여 전자서명 검증을 함으로써 전자서명의 특성인 상호인증과 메시지 무결성보장이 가능하다. 둘째, 메시지에 nonce값을 포함하여 송수신함으로써 메시지를 절취하여 공격하는 재연공격시 nonce값을 확인하여 응답하지 못하도록하여 공격을 방지할 수 있다. 셋째, 기존의 XKMS 2.0에는 클라이언트와 XKMS간의 송수신 메시지에 대한 사항만 명시 되었으나 제안한 명세는 PKI와 XKMS간 메시지 송수신 절차 및 형식과 더불어 XKMS와 PKI의 연동방안에 대한 개념을 포함하여 실제 시스템 설계 및 구현 시 도움이 될 것으로 판단된다.

5. 결 론

본 논문에서는 기존의 XKMS에서는 포함되지 않았던 XKMS와 PKI의 안전한 연동 방안으로서 PKI와 XKMS간의 연동개념 및 상호인증방안을 제안하였고, 메시지 무결성 보장 및 재연공격 방지 방안을 제안하여 실제 XKMS시스템 설계 및 구현 시 보다 보안이 강화된 시스템을 개발하는데 도움을 주고자 하였다.

향후 본 연구를 발전시키기 위해서는 실제 XKMS시스템 설계 및 구현을 통한 효율성 검증이 필요할 것이며 본 논문을 조금 더 발전시키면 웹서비스 클라이언트와 XKMS간의 상호인증 및 메시지 무결성 보장 방안도 연구될 수 있을 것이라 판단된다.

참고문헌

[1] W3C, XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsigcore, 2002. 2.
[2] W3C, XML Encryption Syntax and Processing, http://www.w3.org/TR/xmlenccore, 2002. 12.
[3] W3C, XML Key Management Specification(XKMS) Ver 2.0, http://www.w3.org/TR/xkms2, 2005. 6.
[4] 남길현, 정보시스템 보안론, 국방대학교, 2003. 3.
[5] 홍기용 외, "웹서비스 보안기술 표준화 동향", 정보보호학회지 제14권 제4호, 2004. 8.