제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

인터넷 환경 하에서의 XML 기반의 안전한 메시징 시스템 연구

안경림*, 정진욱**
*한국물류정보통신㈜
**성균관대학교 정보통신공학부
e-mail : krahn@klnet.co.kr

A Study of Secure Messaging System Using XML based on Internet Environment

Kyeong-Rim Ahn*, Jin-Wook Chung**
*KL-Net(Korea Logistics Network)
**School of Information and Communication Engineering, SungKyunKwan University

요 약

사업 영역 확대와 네트워크 발달로 인해 전자상거래(Electronic Commerce)는 점차 국제적 환경으로 확대되고 있으며, 장소나 시간에 구애받지 않고 정보를 전송할 수 있게 되었다. 거래되는 업무가 증가됨에 따라 거래내용, 결제 내용(계좌번호, 카드번호 등), 비밀번호 등 교환되는 정보의 종류도 다양해져 보안의 중요성이 대두되었다. 이에 데이터 사용 효율과 응용 가능성을 높이기 위해 차세대 인터넷 표준으로 대두되고 있는 XML 을 메시지 처리 단위로 정의하고, XML 기반의 인터넷 메시징 시스템인 IMSX (Internet Messaging System based on XML)을 설계하였으며, 보안 위협으로부터 대응하기 위해 암호화(Encryption)와 전자서명(Digital Signature) 등의 메시지 레벨의 응용 보안을 적용하였다. 또한 문서 송신, 문서 수신, 검색, 문서 변환, 템플릿(Template) 제공, 보안 서비스 등을 선정하여 구현하였다

1. 서론

사업 영역 확대와 네트워크 발달로 인해 전자상거래(Electronic Commerce)는 점차 국제적 환경으로 확대되어 가고 있으며, 거래되는 업무가 증가됨에 따라 거래내용, 결제 내용(계좌번호, 카드번호 등), 비밀번호 등 교환되는 정보의 종류도 다양해져 보안의 중요성이 대두되었다.[1][2][3]

그러나 웹 기반의 메시징 시스템은 HTML 의 제한조건때문에 재활용이 불가능하며, 교환되는 데이터가 증가함에 따라 네트워크 상의 보안도 강화되어야 했다.[5] 이에 본 논문에서는 데이터 사용 효율과 응용 가능성을 높이기 위해 차세대 인터넷 표준으로 대두되고 있는 XML 을 메시지 처리 단위로 정의하고, XML 기반의 인터넷 메시징 시스템인 IMSX (Internet Messaging System based on XML)을 설계하였으며, 보안 위협요소로부터 대응하기 위해 메시지 레벨의 응용 보안을 적용하였다. 또한 문서 송신, 문서 수신, 검색, 문서 변환, 템플릿(Template) 제공, 보안 서비스 등을 선정하여 구현하였다.

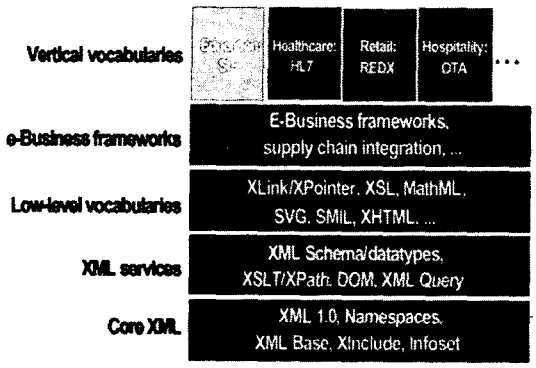
본 논문의 구성을 살펴보면 먼저 제 2 장에서는 기반기술에 대해 설명하였고, 제 3 장에서는 XML 기반의 인터넷 메시징 시스템인 IMSX 의 구조와 제공할 수 있는 서비스 중 몇 가지를 선정하여 구현한 예를 설명하겠다. 마지막으로 제 4 장에서는 결론과 향후 연구과제에 대해 설명하였다.

2. 기반기술

2.1 전자상거래 프레임워크(Framework)

전자상거래 프레임워크란 " 컴퓨터 대 컴퓨터 망을 이용하여 한 기업체의 비즈니스 경계를 넘어 거래 상대방(Trading Partner)과의 상거래를 가능하게 하는 기능(function)을 규정하는 일반적 골격(template)을 의미하며, XML 이 전자상거래에 최대한 활용되기 위해서는 표준화 작업이 이뤄지어야 한다.[3] 전자상거래 표준화 프레임워크는, 특히 XML 기반 Framework 는 다양한 형태로 작업이 진행 중이며, 각 작업마다 나름대로의 특성과 주안점을 가지며, 추

진은 기업, 산업 업종 단체, 비영리 기구 등 다양한 주체에 의해 이뤄지고 있다. 다음 (그림 1)은 XML 기반기술과 XML 프레임워크의 상관관계를 보여주고 있다.



(그림 1) XML 과 프레임워크간의 상관관계

2.2 EDI

전자문서교환(EDI:Electronic Data Interchange) 시스템이란 기업이나 조직간의 상호거래에 필요한 데이터를 전자적으로 상호교환하는 것으로서, 거래 당사자들 사이에 표준화되고 정형화된 문서를 교환하는 것을 의미한다. EDI 를 도입함으로 인해 처리시간 및 비용의 절감, 오류의 감소, 업무 처리절차 감소 등 많은 이점이 발생하였다.[1][2][4] 그러나 인터넷이 도입되고 기업간 거래에서 누구나 사용할 수 있는 거래로 확대됨에 따라 EDI 만으로는 감당할 수 없게 되었다. 이에 따라 인터넷 EDI 시스템이 개발되었으나, 이 또한 고정 태그 사용, 문서 재사용 등 HTML 의 한계로 인한 문제점이 존재한다.

2.3 XML

XML(eXtensible Markup Language : 확장 가능한 마크업 언어)은 사용자가 직접 태그를 정의할 수 있는 확장이 가능한 언어이다.[10][11][12][13] XML 은 이기종 시스템간 호환성과 표준화 기술이라는 점 때문에 인터넷 뿐만 아니라 여러 방면에서 활용할 수 있으며, 특히 전자상거래 분야에서 매우 활용도가 높을 것이다. 또한 전자 카탈로그와 EDI 시스템 등에서 XML 을 활용하고 있으며 그 활용 방면이 점점 넓어지고 있는 추세이다.[7][8][9] 새로운 태그의 의미를 이해하기 위해, 정의한 태그들간의 관계나 문서의 구조 등을 표현하기 위해 DTD (Document Type Definition)가 사용된다. 또 다른 표현 방법인 XML Schema 는 XML 문서 구조와 내용을 정의하는 것으로, DTD 에서 표현할 수 없었던 데이터 타입과 엘리먼트 재사용 등이 가능하다. 즉 XML Schema 는 DTD 를 확장한 모델로서 XML 문서가 가질 수 있는 엘리먼트 타입, 엘리먼트 간의 관계, 각 엘리먼트가 가질 수 있는 타입에 대해 상세히 정의할 수 있다.

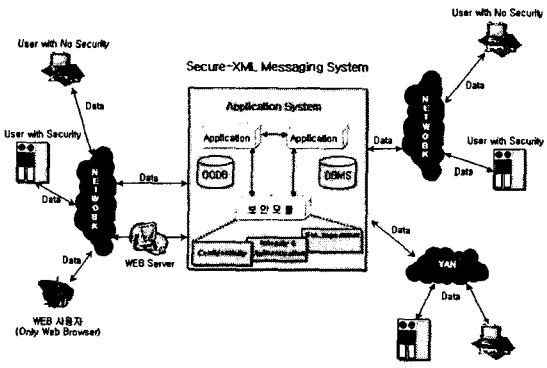
2.4 보안 기술

대칭키 알고리즘은 동일한 대칭키를 사용하여 암호화 및 복호화를 수행한다. 암호화에 사용된 키는 당사자간 동일키를 공유해야 함으로 인해 거래 상대방이 늘어날수록 키 관리에 어려움이 있다. 비대칭키 알고리즘은 암호화와 복호화시 사용되는 키가 서로 다르다. 비밀키는 자신이 보관하며, 공개키는 외부에 공개한다. 사용자들은 자신의 비밀키만 보관함으로 대칭키 알고리즘보다 키 관리가 용이하지만, 상대적으로 키 크기가 커서 처리 시간 및 부하가 걸리게 된다. 그래서 전체 메시지를 암호화하기 보다는 전자서명시 사용된다.[1][2][3]

정보사회에서 활성화되고 있는 전자문서에 작성자의 신원 확인 및 무결성을 보장하기 위해 1999 년 2 월 5 일 법률 제 5792 호에 따라 전자서명법이 제정되었으며, 전자 문서의 안전성과 신뢰성을 확보하고 국가 정보화와 국민 편익 증진을 목적으로 한다. 전자서명은 전자문서를 작성한 자의 신원과 전자문서의 변경 여부를 확인할 수 있도록 비대칭 암호화 방식을 이용하여 전자서명 생성키로 생성한 정보를 의미한다.

3. 시스템 구성 및 구현

인터넷 메시징 시스템인 IMSX 는 3-Tier 구조로서 DB Layer 와 Application Layer, 웹 서버로 구성된다.[5] 먼저 DB Layer 인 Repository 는 저장소로서 XML 문서와 DTD, XSL 등의 템플릿(Template) 정보가 저장된다. 그리고 Application Layer 인 Converter 는 Any-to-Any Formatting 을 목적으로 하여 설계하였으며, 사용자의 통신을 위해 Web Server 와 독립적인 통신 모듈인 PiMex 를 두었다. (그림 2)는 본 논문에서 설계한 인터넷 메시징 시스템인 IMSX 구조이며, 통신 프로토콜은 TCP/IP(인터넷)을 기본으로 한다.



(그림 2) IMSX 구조 및 메시지 흐름

IMSX 시스템은 여러 서비스 중에서 우선적으로 정보 서비스 제공과 메시지 변환 서비스, 그리고 보안 서비스를 선정하여 구현하였다. 정보 서비스로는 문서 송신/수신/검색, 그리고 클라이언트에서의 문서 처리

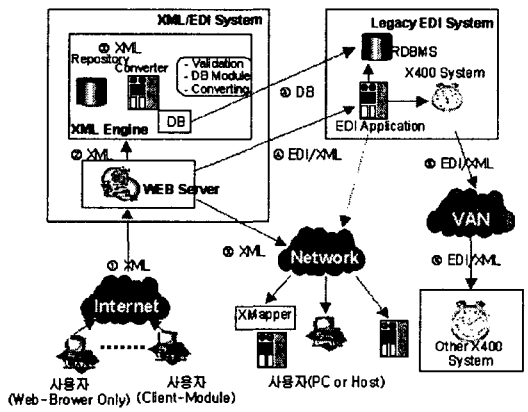
에 대해 구현하였으며, 보안 서비스는 메시지 비밀보장 서비스, 사용자 인 인증 및 메시지 무결성 서비스 그리고 신뢰할 수 있는 제 3 자(CA 또는 중계사업자)와 함께 부인 봉쇄 서비스를 우선 선정하여 구현하였다. 보안 서비스는 암호 알고리즘과 전자서명을 통하여 구현되었으며, 사용된 키(인증서)는 공인인증기관으로부터 발급받아 사용하였다.[1][2]

3.1 정보/변환 서비스

3.1.1 문서 송신, 수신, 검색

사용자가 브라우저를 통해 IMSX 시스템에 접속하여 데이터를 입력하면, 기본적인 검증(Validation Check) 작업이 수행되며, 완료 후 전송버튼을 누르면 클라이언트 단에서 상위 레벨의 검증작업이 행해지며 결과에 따라 XML 문서가 생성되어 IMSX System 으로 전송된다 전송된 문서는 Valid XML 문서인지를 체크하고, 검증(Validation Check, Syntax & Semantic) 작업을 한다. 검증이 완료된 XML 문서는 Repository 에 저장되며 수신자에게 전송한다.

사용자가 문서를 수신받기 위해서는 먼저 IMSX 시스템에 접속하여 수신할 문서 종류와 문서 형태를 선택한다. IMSX System 은 선택한 XML 문서를 Repository 에서 추출하여, XML 을 선택했을 경우는 그대로 전송이 되며, EDI 나 HTML 형태를 선택했을 경우에는 Repository 에서 해당 XSL 을 추출하여 XSLT 를 통해 EDI 나 HTML 형태로 변환하여 사용자에게 전송된다. 다음 (그림 3)은 문서 송신 입력 시의 처리 절차에 대해 보여주고 있다.



(그림 3) 문서 송신 처리 절차

3.1.2 클라이언트측에서의 문서 처리

문서를 수신받은 사용자가 DB 에 저장하는 방법에 대해 설명하겠다. 먼저 XML 문서에 대해 각 태그별 값에 대해 DB Table 필드와 매핑을 한다. 매핑 작업이 완료가 되면 DB 구문에 맞춰 저장한다. 현재는 별도의 프로세스가 클라이언트에 존재하여 수신받은 XML 를 처리하고 있지만, 향후 XML 문서에 비즈니스(프로세싱) 로직을 첨부하여 전송할 수 있는데, 별도의 조작없이 내부 처리를 할 수 있다.

3.2 보안 서비스

3.2.1 메시지 비밀보장 서비스

메시지 비밀보장(Data Confidentiality) 서비스는 불법 노출로부터 데이터를 보호하기 위한 것으로서, 본 논문에서는 국내 비대칭키 표준 알고리즘인 SEED-CBC 128 비트 블록 암호 알고리즘을 사용하였다. 송신자는 전송하고자 하는 메시지에 암호화 키(수신자의 공개키)를 적용하여 암호화 후, 암호문을 수신자에게 전송한다. 수신자는 복호화 키(수신자의 비밀키)를 사용하여 암호문을 복호화한다. 이 때 암호화에 사용된 키는 공인인증기관(CA)으로 발급받은 인증서를 통해 정의된다.

3.2.2 사용자 인증 및 데이터 무결성 서비스

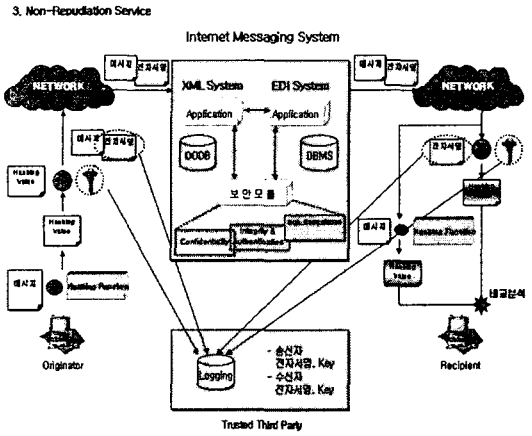
사용자 인증(User Authentication) 서비스는 메시지가 발신자로부터 보내진다는 것을 보장할 수 있는 서비스이고, 메시지 무결성 (Data Integrity) 서비스는 송신자가 전송한 메시지가 수신자가 수신하기 전에 불법 변경이나 수정이 없었다는 것을 보장하는 서비스이다. 본 논문에서는 해쉬 함수로서 160 bit, 4 round SHA1 을 사용하였으며, 암호화 알고리즘으로는 RSA 를 사용하였다. 송신자는 원문에 전자서명을 포함하여 수신자에게 전송하면, 수신자는 송신자의 공개키로 전자서명을 복호화한다. 이 때 복호화된 값(메시지 요약 : Message Digest)과 원문을 송신측과 동일한 해쉬 함수를 적용하여 나온 값(메시지 요약)을 비교한다. 이 두 값이 동일하면 정당한 메시지 발신자로부터 전송되었다는 것과 전송된 메시지가 전송도중 변경없이 전송되었다는 것을 보장할 수 있다.

3.2.3 부인봉쇄 서비스

부인봉쇄(Non-Repudiation) 서비스는 일반적인 전자상거래시 수신자가 수신 사실을 부인하고 미수신 Claim 을 제기하거나 수신자가 수신받은 메시지 내용이 송신된 내용과 다르다거나 송신 사실을 부인하는 시도로부터 보호하기 위해서 제공되는 서비스이다. 근거자료 보관 방법은 각자의 시스템에 전자서명을 보관하거나 또는 신뢰할 수 있는 제 3 자에게 저장할 수 있다. 본 논문에서는 디지털 메커니즘을 사용하는 사용자 인증 및 메시지 무결성 서비스에다가 전자서명 및 키를 신뢰할 수 있는 제 3 자가 보관하는 방식으로 구현하였다. 다음 (그림 4)는 부인봉쇄 서비스 절차를 보여주고 있다.

전자서명 메커니즘에 의해 먼저 송신자는 메시지에 해쉬 함수를 적용하여 나온 메시지 요약(Message Digest)에 자신의 비밀키로 암호화하여 전자서명을 얻는다. 원문에 전자서명을 포함하여 수신자에게 전송하면, 수신자는 송신자의 공개키로 전자서명을 복호화한 복호화한다. 이 때 복호화된 값(메시지 요약 : Message Digest)과 원문을 송신측과 동일한 해쉬 함수를 적용하여 나온 값(메시지 요약)을 비교한다. 이 두 값이 동일하면 정당한 메시지 발신자로부터 전송되었다는 것과 전송된 메시지가 전송도중 변경없이 전송되었다는 것을 보장할 수 있다. 또한 송신자는 메시지를 송신하기 전에 생성된 전자서명을 제 3 자에게 제출하고,

수신자 또한 수신한 전자서명을 제출한다. 저장된 전자 서명은 분쟁 발생시 증거자료로서 사용된다.



(그림 4) 부인봉쇄 서비스

4. 결론

통신 환경과 인터넷의 발달로 인해 전자상거래가 점차 광범위하게 시행되어, 단순 메시지 전송이나 정보 조회에 불과하던 기능에서 상거래 기능까지 포함하게 되었다. 이렇듯 종이로 처리되던 업무를 점차 전자적으로 전송하면서 표준화된 메시지 형태에 대한 요구사항이 도출되어, EDI 나 XML 등이 정의되어 사용되고 있다. 또한 거래 내용, 개인 정보, 비용(계좌번호, 카드 번호 등) 정보 등 메시지 종류도 다양해지면서 보안에 대한 필요성이 중요시되고 있다. 이를 위해 본 논문에서 제안한 인터넷 메시징 시스템인 IMSX 는 인터넷 환경 하에서 안전하게 메시지를 전송하기 위해 제안된 시스템으로서, 정보 제공 서비스, 문서간 변환 서비스, 그리고 여러 보안 서비스 중 메시지 비밀보장, 사용자 인증 및 메시지 무결성 그리고 부인불능 서비스를 선정하여 구현하였다.

향후 연구과제로는 전자 지불과 전자 카탈로그(Catalog) 등 다양한 상거래 분야와 접목할 수 있도록 시스템을 확장하겠다. 또한 유선 네트워크를 환경만을 고려하여 설계되었으나, 무선(Wireless) 통신까지 지원할 수 있도록 하겠다.

참고문헌

[1] 성균관대, " EDI 시스템 시큐리티 선행기술 연구" 한국통신 최종 연구 보고서, 1993

[2] 안경림, " OSI 환경을 위한 EDI 보안서비스요소의 설계 및 구현" , 논문, 1994

[3] 한국전산원, " 전자상거래를 위한 보안 기술 체계 및 요소 기술에 대한 이해" , 1999

[4] 강은숙, " e-SCM 을 기반으로 한 철도물류정보 시스템의 무선인터넷 도입방안에 관한 연구" , 논문, 2000.

[5] 안경림, 박상필, 임병찬, 강은숙, 조갑성, " XML 기반의 철도물류정보 System 설계 및 구현" , 한국 SI 학회 창립기념학술대회

[6] Dan Chang&Dan Harkey, " Client/Server Data access with Java and XML" , Wiley & Sons Inc., Canada, 1998

[7] Sean McGrath, " XML Processing with Python" , Prentice-Hall Inc.

[8] David Webber, " XML/EDI Perspectives" , Japan.

[9] http://www.xmledi-group.org/xmledigroup/guide.htm - "Guidelines for using XML for Electronic Data Interchange"

[10] http://www.w3.org/TR/REC-xml - Extensible Markup Language (XML) 1.0 Specification 10. Feb 1998, Tim Bray, Jean Paoli, C. M. Sperberg-McQueen

[11] http://www.w3.org/TR/xsl/ - Extensible Style sheet Language (XSL) Version 1.0 27 Mar 2000, Sharon Adler, Anders Berglund, Jeff Caruso, Stephen Deach, Paul Grosso, Eduardo Gutentag, Alex Milowski, Scott Parnell, Jeremy Richman, Steve Zilles Last Call Ends 30 Apr 2000.

[12] http://www.w3.org/TR/xslt - XSL Transformations (XSLT) Version 1.0 16 Nov 1999, James Clark

[13] http://www.w3.org/TandS/QL/QL98/pp/xql.html - XML Query Languange(XQL) September 1998 to the XSL Working Group