論文
2-9-12

안전한 XML 메시징 시스템 설계 및 구현 (The Design and Implementation of Secure XML Messaging System)

이 영 교* 안 경 림**
(Young-Gyo Lee) (Kyeong-Rim Ahn)

요 약

전자상거래가 활성화되면서 상거래 기능과 거래되는 업무가 증가함에 따라 교환되는 메시지도 다양하게 되어, 개인정보, 결제정보(계좌번호, 카드번호, 비밀번호 등), 개인정보 등, 이러한 메시지에 대한 보안이 요구된다. 그래서 본 논문에서는 인터넷 환경 하에서 안전하게 메시지를 전송하기 위해 암호와 전자서명을 적용한 안전한 XML 메시징 시스템인 Secure-XML Messaging 시스템(S-XMS)은 위해 제안하였으며, 여러 보안 서비스 중 메시지 비밀보장 서비스, 사용자 인증 서비스, 메시지 무결성 서비스, 부인불능 서비스를 선정하여 구현하였다.

ABSTRACT

Security is very important at EC(Electronic Commerce) Environments. The reason is that exchanged data(that is user private information(accounts, card-no, password), transaction items, etc) is various and is very sensitive. In this paper, we propose the Secure-XML Messaging System(S-XMS) which is implemented to support Message Level Security, Encryption and Digital Signature. And we implement Message Confidentiality Service, User Authentication & Message Integrity Service and Non-Repudiation Service among the various Security Services.

1. 서론

전자상거래가 활성화되면서 상거래 기능과 거래되는 업무가 증가함에 따라 교환되는 메시지도 다양하게 되어, 개인정보, 결제정보(계좌번호, 카드번호, 비밀번호 등), 개인정보 등, 이러한 메시지에 대한 보안이 요구된다. 더욱이 인터넷을 기본으로 하는 환경으로 변화함에 따라 네트워크 상의 보안도 중요시 되고 있다.

이를 위해 본 논문에서 제안한 XML 메시징 시스템인Secure-XML Messaging 시스템(S-XMS)은 인터넷 환경 하에서 안전하게 메시지를 전송하기 위해 설계하였으며, 여러 보안 서비스 중 메시지 비밀보장 서비스, 사용자 인증 서비스, 메시지 무결성 서비스, 부인불능 서비스를 선정하여 구현하였다.

* 정회원 : (주)에임텍 과장
** 정회원 : 한국 물류 정보 통신 연구소 과장

논문접수 : 2001. 9. 13.
심사완료 : 2001. 9. 22.

본 논문의 구성을 살펴보면 먼저 제 2장에서는 전자상거래 환경 하에 존재하는 보안 위협요소와 이에 대응하기 위한 보안서비스에 대해 살펴보고, 제 3장에서는 보안 서비스를 구현하기 위해 사용될 수 있는 보안에 대해 설명하겠다. 제 장에서는 Secure-XML 메시징 시스템 설계와 서비스 구현예에 대해 설명하겠으며, 마지막으로 제 5장에서는 결론과 향후 해결해야 할 문제에 대해서 언급하겠다.

2. 보안 기술 동향

요즘 활발히 시행되고 있는 전자상거래는 인터넷을 기반으로 서비스되고 있는데, 인터넷이 갖는 기본적인 취약성 때문에 거래 내용, 자기 정보, 비용(계좌번호, 카드 번호 등) 정보, 비밀번호 등의 정보가 쉽게 노출될 수 있다. 현재 전자상거래 환경은 국가간, 조직간, 개인 간 거래를 위해 연결되어 있을 뿐 아니라 사용자의 인적 사항과 거래에 따른 지불 정보가 전송되고 있어 더욱 위협에 노출되어 있다. 전자상거래에서 발생하는 보안상의 위협 요소와 이에 대응하는 보안 서비스 요소를 살펴보면 다음과 같다.[1][2][3]

2.1 보안 위협 요소

2.1.1 도청(Eavesdropping)

네트워크를 도청하여 전송되는 메시지를 복제(Counterfeit , Replication)한다.

2.1.2 위장(Masquerade)

침입자가 합법적인 사용자인 것처럼 시스템에 접근하여 메시지의 수신에 대해 정당한 수신자인 것처럼 거짓 응답을 할 수 있고, 거짓요청을 하여 임의의 메시지가 제출되게 할 수도 있다.

2.1.3 메시지 변조

의도된 수신자에 대한 정보, 라우팅 정보, 또는 그 외 데이터가 감지되지 못한 채 분실 또는 변경될 수 있으며, 도청한 메시지의 내용을 변경하여 재사용하거나 수신된 메시지를 변경하여 저장할 수 있다.

2.2 보안 서비스

2.2.1 메시지 비밀보장

내용 비밀보장을 제공하기 위해, 발신자는 메시지 내용을 암호 알고리즘과 키를 사용하여 암호화한다. 암호 알고리즘과 키는 상호 협의하여 사용할 수 있다.

2.2.2 메시지 무결성 및 사용자 인증

사용자 인증 및 메시지 무결성은 전자서명과 암호화를 통해 제공되며, 암호/서명키(즉, 미리 설정되고, 공유된 대칭키, 발신자 개인키, 임의로 생성된 대칭키)가 정의된다.

2.2.3 부인불능 서비스

"송신자가 의도된 수신자로의 메시지 전송을 요구하였다"는 것이나 "수신자가 메시지 수신하였다"는 부인할 수 없는 증명을 제공하는 것으로, 증명 서비스보다 강력하다.

2.3 보안 알고리즘

2.3.1 대칭키 알고리즘

대칭키 알고리즘은 동일한 대칭키를 사용하여 암호화 및 복호화를 수행하며, 변환 방법에 따라 블록 암호 알고리즘과 스트림 암호 알고리즘으로 구분된다.[2][3]

블록 암호 알고리즘은 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변경하는 방식으로 암호화 및 복호화 과정을 수행한다. 대표적인 알고리즘으로는 미국의 DES(Data Encryption Standard), Triple-DES, Skipjack, 유럽의IDEA(International Data Encryption Algorithm), 일본의 FEAL(Fast Data Encipherment Algorithm), MISTY 등이 있다. 스트림 암호 시스템은 군사 및 외교용으로 널리 사용되고 있으며, 일부 상용으로도 활발히 사용되고 있다. 또한 이동 통신 환경에서 구현이 용이하고, 안전성을 수학적으로 엄밀하게 분석할 수 있는 장점 등으로 인하여 이동 통신 등의 무선 통신 데이터 보호에 적합하다.

2.3.2 비밀키 알고리즘

비밀키 알고리즘은 암호화와 복호화시 사용되는 키가 서로 다르며, 공개키 알고리즘으로 불리운다. 사용되는 키는 키 생성 알고리즘에 의해 두 개의 키가 생성되는데 하나는 비밀키로서 자신이 보관하며, 다른 하나는 공개키로서 외부에 공개한다. 송신자는 메시지를 암호화 하여 전송하기 위해 수신자의 공개키로 암호화하여 전송하고, 수신자는 자신의 비밀키로 복호화한다. 지금까지 발표된 것으로는 인수 분해의 어려움을 이용한 RSA(Rivest, Shamir, Adleman) 알고리즘, Knapsack 문제를 이용한 Merkle-Hellman Knapsack 알고리즘, Graham- Shamir 알고리즘, 선형 오류 정정 부호를 복호화할 때의 어려움을 이용한 McElieced 암호화 방식, 최근에 가장 큰 관심을 모으고 있는 타원 곡선 암호 시스템(ECC : Elliptic Curve Cryptography) 등이 있다.[2][3]

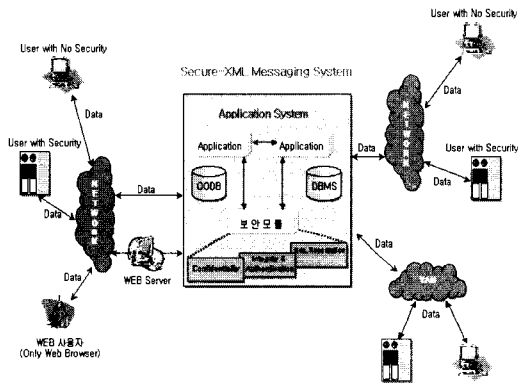
3. 시스템 설계 및 구현

현재 시행되고 있는 전자상거래 시스템은 인터넷을 기반으로 하고 있기 때문에 도청, 위장, 메시지 변조 등과 같은 보안 위협에 노출되어 있다. 상거래시 교환되는 데이터는 자기 정보, 지불 정보, 거래 내역 등과 같은 개인과 기업의 중요 데이터이므로 더욱 보안이 요구된다. 그러므로 본 논문에서는 전자상거래 시스템에서 제공될 수 있는 보안 서비스 중 메시지 비밀보장 서비스, 사용자 인증 및 메시지 무결성 서비스 그리고 신뢰할 수 있는 제 3자(CA 또는 중계사업자)와 함께 부인불능 서비스를 선정하여 우선 구현하였다. 이 서비스들은 암호 알고리즘과 전자서명을 통하여 구현되었으며, 사용된 키(인증서)는 공인인증기관으로부터 발급받아 사용하였다.[4]

3.1 시스템 구조 및 메시지 흐름도

안전한 메시징 시스템인 Secure-XML 메시징 시스템은 인터넷을 기반으로 하여 설계된 시스템으로서 교환되는 메시지는 XML을 기본으로 하였다. 구현된 보안 서비스는 메시지 비밀보장 서비스, 사용자 인증 및 메시지 무결성 서비스, 부인 불능 서비스이고, 이러한 서비스를 위해 보안 모듈이 Component로서 구현되었다. 이 때 사용되는 키는 사용자별로 구분되어 관리된다. 부인불능 서비스를 위해 전송되는 메시지의 전자서명은 정부에서 고시한 기간동안 시스템 내에 보관된다.

다음 [그림 1]은 Secure-XML 메시징 시스템 구조와 교환되는 메시지의 흐름을 보여주고 있다.



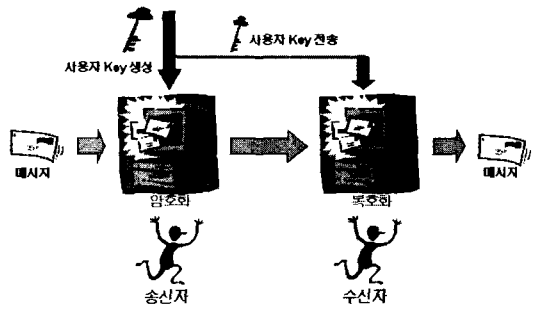
[그림 1] S-XML 메시징 시스템 구조

[Fig. 1] S-XML messaging system structure

3.2 구현 보안 서비스

3.2.1 메시지 비밀보장 서비스 (Data Confidentiality)

메시지 비밀보장 서비스는 불법 노출로부터 데이터를 보호하기 위한 것으로서, 본 논문에서는 국내 비대칭키 표준 알고리즘인 SEED-CBC 128 비트 블록 암호 알고리즘을 사용하였다. 다음 [그림 2]는 비밀보장 서비스의 처리절차를 보여주고 있다.



[그림 2] 메시지 비밀보장 서비스
[Fig. 2] Data Confidentiality Service

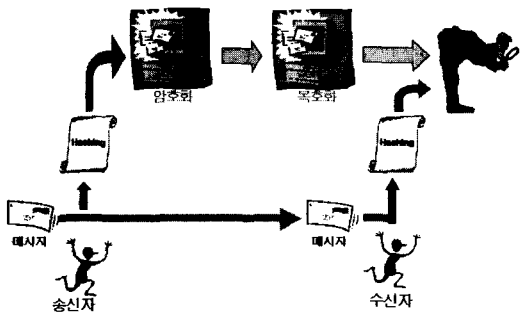
먼저 송신자는 전송하고자 하는 메시지에 암호화 키(수신자의 공개키)를 적용하여 암호문을 생성하고, 수신자에게 전송한다. 수신자는 복호화 키(수신자의 비밀키)를 사용하여 암호문을 복호화한다. 이 때 암호화 때 사용된 키는 인증기관(CA)으로 발급받은 인증서를 통해 정의된다.

3.2.2 사용자 인증(User Authentication)과 데이터 무결성(Data Integrity) 서비스

사용자 인증 서비스는 메시지의 발신자로부터 보내진다는 것을 보장할 수 있는 서비스로서 송신자는 자신의 비밀키로 암호화하여 전송하고, 수신자는 송신자의 공개키로 복호화한다. 메시지 무결성 서비스는 송신자가 전송한 메시지가 수신자가 수신하기 전에 불법 변경이나 수정이 없었다는 것을 보장하는 서비스이다. 이 두 서비스는 디지털 서명 메커니즘으로 구현되며, 암호화 전에 메시지를 블록 단위의 길이로 나누어 해쉬 함수를 수행한다.

다음 [그림 3]은 사용자 인증 서비스와 메시지 무결성 서비스 처리 절차를 나타내고 있다. 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 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.

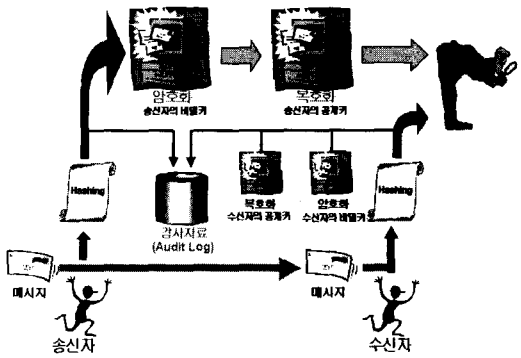


[그림 3] 사용자 인증 및 무결성 서비스
[Fig. 3] User Authentication & Data Integrity Service

3.2.3 부인불능(Non-repudiation) 서비스

일반적인 전자상거래시, 수신자가 수신 사실을 부인하고 미수신 Claim을 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 3자에게 저장할 수 있다. 다음 [그림 4]는 부인불능 서비스 절차를 보여주고 있다. 이 서비스는 사용자 인증과 메시지 무결성 서비스와 동일한 메커니즘을 통해 제공될 수 있다. 송신자는 메시지를 송신하기 전에 생성된 전자서명을 제 3자에게 제출하고,

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



[그림 4] 부인불능 서비스

[Fig. 4] Non-repudiation Service

4. 결론

소규모로 시행되던 전자상거래가 점차 광범위하게 시행되어, 예전의 단순 메시지 전송이나 정보 조회에 불과하던 기능도 점차 off-line으로 행해지는 상거래의 기능까지 포함하게 되었다. 이렇듯 전자상거래가 도입되면서 표준화된 메시지 형태에 대한 요구사항이 도출되었다. 업무가 증가함에 따라 거래 내용, 개인 정보, 비용(계좌번호, 카드 번호 등) 정보 등 메시지 종류도 다양해지면서 보안에 대한 필요성이 중요시되고 있다. 그러나 물리적 보안(방화벽)이나 단순 인증(Simple Authentication)만으로는 인터넷을 기반으로 하는 전자상거래 시스템 내에 존재하는 위협요소에 대해 방어할 수 없어 보다 강력한 보안 정책이 요구되고 있다. 이를 위해 본 논문에서 제안한 안전한 XML 메시징 시스템(Secure-XML Messaging System)은 인터넷 환경 하에서 안전하게 메시지를 전송하기 위해 설계되었으며, 여러 보안 서비스 중 메시지 비밀보장 서비스, 사용자 인증 및 메시지 무결성 서비스 그리고 부인불능 서비스를 선정하여 구현하였다.

향후 연구과제로는 현재 트랜잭션(Transaction) 위주로 되어 있으나, 전자 지불과 전자 카탈로그(Catalog) 등 다양한 분야와 접목할 수 있도록 하겠다. 또한 유선 네트워크를 이용하는 전자상거래 환경만을 지원하고 있으나 무선(Wireless) 통신 환경에서도 지원할 수 있도록 하겠다.

※ 참고문헌

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

[2] 안경림, OSI 환경을 위한 EDI 보안서비스요소의 설계 및 구현, 석사 학위 논문, 1994.

[3] "전자상거래를 위한 보안 기술 체계 및 요소기술에 대한 이해" 한국전산원, 1999, 6

[4] 안경림, 박상필, 안정희, "인터넷을 기반으로 하는 메시징 시스템(XML/EDI System) 설계 및 구현", 한국정보거래(CALS/EC)학회지 제 5권 제 2호, 2001. 3, pp.101-112.

[5] 이영교, 안경림, 안정희, "Java를 기반으로 하는 Internet Messaging System(XML/EDI system) 설계 및 구현", 한국OA학회논문지 제6권 제2호, 2001.6. pp.78-83

[6] 안경림, 백혜경, 임병찬, 이영교, "인터넷을 기반으로 하는 메시징 시스템(XML/EDI System) 설계 및 구현", 한국정보거래(CALS/EC)학회지 제 5권 제 2호, 2001. 3, pp.101-112.

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

[8] Sean McGrath, Sean McGrath : XML processing with Python, Prentice-Hall Inc.Upper saddle River, NJ, 2000.

[9] David Webber, David Webber: XML/EDI Perspectives, Japan, 1998.

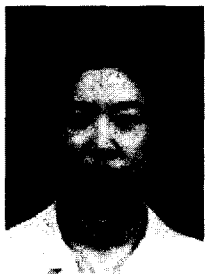
[10] http://www.xmledi-group.org/xmledigroup /guide.htm-"Guidelines for using XML for Electronic Data Interchange"

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

이 영 교

1986년 한양대학교 전자공학과 (공학사)
1991.6 한양대학교 전자공학과 대학원(공학석사)
1993.8~1998.9 대우통신 종합연구소 선임연구원
1999.2~2001.6 LG 전자 중앙연구소 선임연구원
2001.9~현재 (주)에임택 과장
관심분야: 정보 통신 보안 및 전자상거래, 트래픽제어

안 경 림



1993.2 충북대학교 컴퓨터공학과(공학사)
1995.2 성균관대학 정보공학과 대학원(공학석사)
1995.1~현재 한국 물류 정보 통신 연구소 과장
관심분야: 정보 통신 보안 및 전자상거래, 트래픽제어