UN/EDIFACT메시지의 EDI 보안알고리즘

정용규
서울보건대학 전산정보처리과
ygjung@shjc.ac.kr

EDI Security Algorithm on UN/EDIFACT Messages

Yong-Gyu JUNG
Dept. of Computer Inform., Seoul Health College

요 약

전자문서교환(EDI, Electronic Data Interchange)은 기업과 기업간에 컴퓨터와 컴퓨터의 통신을 통하여 필요한 거래문서를 구조화된 형식으로 교환하여 업무를 처리하는 방식을 말한다. 이러한 전자문서의 유통은 여러 위협요소로부터 완전히 해방되지는 못한다. 본 연구에서는 향후 국내에서 발생될 위협요소 중 우선적인 보호가 요구되는 것으로 메시지 노출로 인한 프라이버시 침해 및 중요 내용의 노출문제와 메시지 수정 문제 및 발신처 인증 문제, 그리고 수신자의 수신사실에 대한 부인을 위협요소로 선정하였다. 또한, 이를 막기 위한 보안서비스를 메시지 비밀보장, 무결성, 메시지 발신처 인증 및 수신내용 부인불능 등을 선정하여 이들의 구현방안을 제시하였다.

1. 서론

컴퓨터시스템 또는 컴퓨터망에서의 메시지 처리과정에는 정보에 대한 불법적인 접근(Access), 도청(Eavesdropping), 수정(Modifying), 삭제(Deleting), 재전송(Replying), 삽입(Inserting), 순서변경, 미확인 발신자 및 수신자 등의 위협을 내포하게 된다. 이에 대한 EDI 시스템상의 보안서비스는 X.435등 국제적 표준에서 정한 보안서비스를 분석하고 적용해야 한다. 대부분 업체는 CCITT X.400 MHS(Message handling System)와 CCITT X.500 디렉토리 서비스의 장점과 표준을 따르는 플랫폼 제품에 초점을 맞추고 있어 기업의 정보자원에 대한 보안망을 형성할 필요성이 높아지고 있다. 따라서, EDI소프트웨어의 개발과 표준화 등과 아울러 EDI 보안 문제도 단기적으로 해결해야 할 과제들이다. 국내 일부 기업 및 학계에서 EDI시스템에 대한 모듈별 연구를 추진해 왔으나 아직까지는 미진한 상태이며 향후 국내 소프트웨어 산업의 활성화 및 자체기술 축적의 측면에서도 가능한 각 기업의 특성에 맞는 분야의 기술개발이 필요하다.

EDI를 사용함으로써 많은 효과를 가져올 수는 있으나 반면에 위협요인에 대처할 보안이 없을 시는 기업의 손실을 크게 초래할 수도 있다. 그것은 LAN에서나 공중망 통신에서 개방형 상호접속 (OSI: Open Systems Interconnection)의 표준화 플랫폼을 사용하고 있기 때문에 보안이 더욱 요구되어진다. 본 논문에서는 공중통신망에서의 데이터 보안에 관련한 기술적 방법과 EDI 메시지 레벨에서의 보안 알고리즘에 관하여 살펴본다.

2. EDI보안 서비스

2.1 비밀보장 서비스

하위 계층에서 이러한 보안서비스의 실행에 필요한 데이터가 대등 실체 인증 보안 서비스를 제공하기 위한 접속비밀성(Connection Confidentiality), 메시지의 발신자와 수신지만이 메시지의 내용을 알수 있다는 확신을 제공하는 내용비밀성(Content Confidentiality), 그리고 이중봉투(Double Enveloping)기술을 사용하여 완전한 메시지를 다른 메시지의 내용이 되도록 MTS의 임의의 부분으로부터 주소정보를 감추기 위한 메시지 흐름 비밀성(Message Flow Confidentiality)이 있다.

2.2 인증 및 무결성 서비스

인증서비스에는 크게 3가지를 들수 있는데, 모든 관계된 실체들에 대해서 메시지, 프로브, 리포트의 발신처에 대한 확증을 제공하는 데이터 발신처 인증 보안 서비스, 그리고 메시지가 수신자에게 배달되기 위해서 MTS가 확실하게 수신하였다는 사실을 메시지의 발신자에게 제공하고, 제출증명 보안요소를 이용하여 제공되어 질수 있는 제출증명 보안서비스, 마지막으로 메시지가 의도한 수신자에게 배달되었다는 확신을 메시지의 발신자에게 제공하고 배달증명 보안요소를 이용하여 제공되어질수 있는 배달증명 배달서비스를 들 수 있다.

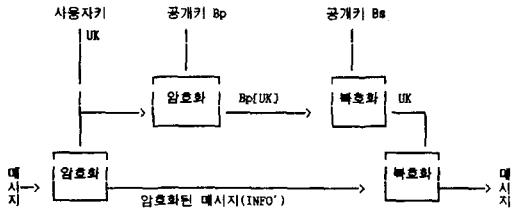
2.3 부인방지 서비스

메시지 생성자가 메시지 보낸 사실에 대해 부인하는 것을 막는 근원 부인방지 서비스 (Non-Repudiation of Origin Service)와 메시지 수신자가 메시지의 배달 사실에 대해 부인하는 것을 막는 배달 부인방지 서비스 (Non-repudiation of Delivery Service)등이 있다.

3. EDI 보안알고리즘의 설계

3.1. 비밀보장 알고리즘

메시지의 불법 노출로부터 데이터를 보호하기 위한 것으로 사용되는 암호 알고리즘은 송신측에서 사용한 키를 수신측의 공개키를 사용하여 암호화시켜 전송하게 함으로써 수신측에서는 메시지를 암호화한 키를 알거나 보관할 필요가 없게 하면 된다. [그림1]에서 보는 바와 같이 사용자 키는 수신측 공개키에 의해 암호화되어 전송되며 수신측은 수신측의 비밀키를 이용하여 사용자 키를 복호화한 후 이 키를 이용하여 메시지를 복호화 하게 한다.

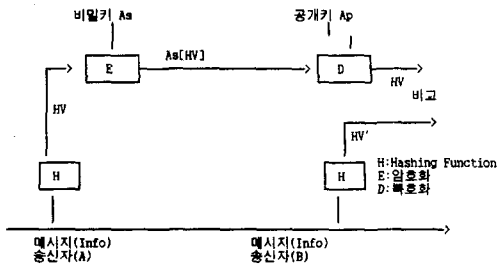


[그림 1] 비밀보장 알고리즘

3.2 인증 및 무결성 알고리즘

발신처 인증 서비스는 메시지의 발신자로 부터 보내진다는 것을 보장할 수 있게 한다. 즉, 발신자는 자기만이 알고 있는 비밀키를 사용하여 암호화하는데 이 때 다른 어떤 사람도 발신자의 비밀키를 알 수 없다. 그리고 수신측에서는 공개키로서 복호화 시킴으로 발신처를 증명할 수 있게 된다.

[그림2]에서 보는 바와 같이 먼저 송신측에서 Hashing함수를 수행하여 얻어진 값 HV를 송신측의 비밀키 As로 서명된 정보를 메시지 헤더에 부가하여 수신측에 보내면, 수신측은 서명된 정보를 공개키 Ap로 보호화시켜 HV를 얻게 된다. 그다음 송신측으로부터 메시지를 동일한 Hashing 함수를 이용하여 HV'를 구하여 송신측으로부터 수신된 HV의 값과 비교한다. 만약 이 값이 같다면 정당한 발신자에게서 온 것을 보장함과 동시에 변경없이 보내졌다는 것을 보장할수 있게 된다.



[그림 2] 인증 및 무결성 알고리즘의 처리 절차

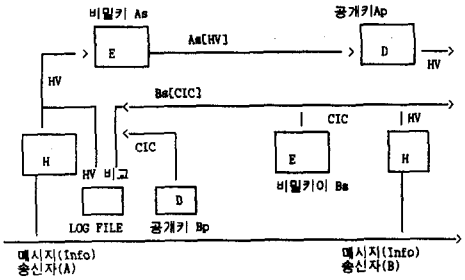
```
UNH+326+PAYORD:1:911:RT'
SEC+AUT++HEX+AS8'
NAD+MS+++MR.SMITH,COMPANY A'
NAD+MR+++BANK A'
RFF+SSN:001'
DTM+STS:940409135950:202'
ALG+OSY:1+KYN+MAC-KEY1'
SLK+S+1'
BGM+450+AZ341234+137:940405:101'
NAD+BE++COMPANY'
CTA++MR.JONES,SLAES'
FII+OR+00387806:COMPANY A+603000:154+132'
FII+BF+00663151+201827:154+132'
DTM+203:940414+101'
MOA+7+9:54345,10:GBP'
DOC+380+62345'
SLK+T+1'
RST+C1FFA1BC'
UNT+19+326'
```

[그림 3] 인증및 무결성을 위한 메시지 예

3.3. 수신내용 부인봉능 알고리즘

청구서 및 대금지불등과 같은 메시지를 받은 수신자가 수신 자체를 부인하고 미수신 Claim을 제기하는 행위이다. 이런 위협을 메시지 발신자가 봉쇄하기 위한 것이 바로 수신내용 부인봉능(Non-repudiation of Receipt) 알고리즘이다. 수신내용 부인봉능은 디지탈서명을 하기 전 송신측의 EDIM (EDI Message)내 Request 필드에 PN 또는 NN을 요청하고 Notification Security 필드를 Proof로 Set시키는 제어과정을 먼저 거치게 된다. 그리고 난 다음 디지탈서명 과정을 거친다. 즉, 메시지 내용이 Hashing 함수를 거친 후 그 값을 서명하여 자체 로그파일에 수록한 다음 수신측으로 전송한다. 수신측에서는 수신된 EDIM이 PN 또는 NN으로 set되어 있으면 EDIM을 생성하기 위해 메시지 내용을 Hashing한 결과값(CIC)을 수신측의 비밀키로 암호화하여 EDIM에 Bs(CIC) B측의 공개키로서 복호화시켜 이 메시지 내의 CIC와 이미 로그파일에 수록된 HV의 값을 비교하여 성

공적으로 수행되었을 경우 수신측이 내용을 받았다는 것을 확인한 후 로그파일에 이 EDIM을 저장시켜 두고 나중에 문제가 발생시 수신자의 수신사실에 대한 부인을 봉쇄하는 근거자료로 제시한다.



[그림 4] 수신내용 부인불능 알고리즘 처리절차

```
UNH+326+PAYORD:1:911:RT'
SEC+NRO+NAK+HEX+AS8'
RFF+SSN:202'
ALG+OHA:52'
CER+00000001++HEX+AS8+931+PK1++DAT:2B:COM:3A:SEG:27
   :REL:3F'
NAD+OW++MR.SMITH+COMPANY A'
NAD+AX+++AUTHORITY'
DTM+273:940101941231:717'
ALG+OSG:20+EXP:00010001:MOD:CA056F9C89708200E822A
   8A19BC6ADD430807705DE2D5AFA7934F63EA8E7C280379
   C02DA758799F34F2C0D1C2747F98E43A1EAA4BE8195FC24
   A17BE70446F95F:MLN:0512'
ALG+IHA:52'
ALG+ISG:20+EXP:00010001:MOD+FC5959DE40BF4DFB13930
   E7FF703FB6089864535F328981CE1CFDF43A010DB79955CA
   8171FC5D463A488C5E5227E8F9BDD562EE4E23BD3F29827
   A53233596341:MLN:0512'
DTM+CGT+931215141200:202'
RST+C080209FC7BEF4EAF589CA5366DC609B5F1729C8FE3A56
   A314108E3C1620B0C0C2E42F007A227A7809783262CB9A
   E5717B4096695FCC774F3FCCB8E8D6D2BE0AE'
SLK+S+1'
BGM+450+AZ341234+137:940405:101'
NAD+BE++COMPANY B:WEST DOCK:MILFORD HAVEN'
CTA++MR.JONES,SALES'
FII+GR+00387806:COMPANY A+603000:154+132'
FII+BF+00663151+201827+154+132'
DTM+203+940414:101'
MOA+7+9:54345,10:GBP'
DOC+380+62345'
SLK+T+1'
RST+6BD7DC037A28325075D51B22A1EF46FB651CD3244A86D7
   C4130E8EB7F7A9CC6EBF750A7172478F2033715C44662DC7
   C212F734B5AB814719717A758F2C04E1A3'
UNT+25+326'
```

[그림 5]수신내용 부인불능을 위한 메시지 예

4. 결론

본 연구에서 보안에 필요한 메시지를 독립적으로 구성하여 Segment와 Element에 보안 항목을 기입한 하나의 메시지형태를 갖는 표준 보안 메시지 설계와 보안 서비스를 메시지의 예를 들어 구현하였다. 이렇게 함으로써 사용자 레벨에서 보안에 필요한 메시지의 구성을 제작할 수 있고 난발도 막을 수 있다. UN에서 권고한 메시지 레벨에서의 보안의 구현은 알고리즘을 공개하고 키를 관리하는 현대적인 보안의 경향을 따르는 것이다. 이런 방법으로 본 연구에서는 샘플 메시지를 만들었고 아울러 보안에 관련한 서비스를 구현하기 위한 보안의 알고리즘도 설계하였다.

본 연구에서 구현한 알고리즘의 성능을 측정하고 효과를 분석하기에는 어려움이 많지만 보안이 필요한 항목에 단순한 디지털서명만 의존하는 보안의 형태에서 벗어나 광범위하고 표준화된 보안의 메시지를 만드는 것은 향후 보안에 필요한 항목을 추가하고 변경하는데 유용할 것이며 보안의 알고리즘 또한 보안의 서비스를 추가시 융통성을 부여할 수 있어 응용하는데 많은 도움이 될 것이다.

예상되는 문제점으로, 보안 서비스를 포함한 메시지를 수신측에 전송하여 수신증명서가 발신측에 도달하는데 많은 시간이 소요될 수 있으며 이는 키의 길이가 크고 계산 량이 많아서 연유한 것이므로 향후 적절한 보안의 적용을 위하여 간략히 구현하는 방안을 연구해야 할 것이다. 다시 말하면 키의 길이를 적게 하면 만족할 만한 효과를 줄 수 있으나 어느 정도의 키 길이가 보안 강도 면에서 안전한지는 사용자의 요구와 보안의 환경에 매우 깊이 좌우될 것이다.

참 고 문 헌

[1] C.P Fleeger, Security in computing, Prestice Hall, 1989

[2] D.W.Davies, W.L.Price, Security for computer network, 2nd ed. John Wiley & Sons, 1989

[3] 전산원,전산망 기술및 표준화 심포지움, p.258, 1992

[4] TRADE/WP.4, UN/EDIFACT Message level Security, 1998

[5] TRADE/WP.4, UN/EDIFACT Security Implementation Guidelines, 1998. 2

[6] Richard Hill, EDI and X.400 using Pedi,Technology Appriaisals, 1999

[7] Jenifer Seberry and Josef Pieprzyk, Cryptography An Introduction to computer Security, Prentice-Hall, 1999