제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

Web 기반 기업 Application 시스템을 위한 보안환경 설계 및 구현

정경희*, 신동규**
*세종대학교 정보통신학과
**세종대학교 컴퓨터공학과
e-mail : khee@nate.com , shindk@sejong.ac.kr

Design and Implementation for Web based Enterprise Application System

Kyung-Hee Jeong*, Dong-Gyu Shin**
*Dept. of Computer Communication, Se-Jong University
**Dept. of Computer Engineering, Se-Jong University

요 약

인터넷을 기반으로 기업 활동이 점차로 넓어지면서, 동적이면서 실시간의 데이터를 제공하기 위하여 거미줄처럼 여러 개의 시스템이 연계되기도 하고, ERP, CRM, EAI 등으로 기업 내 Application 을 통합하기도 한다. Backend System 의 통합으로 얻을 수 있는 기대효과에 맞서서 이의 인터넷 서비스 위험은 더 커져 정보 보안 문제가 중요한 이슈가 되었다.

이에 본 논문에서는 웹 기반 사용자의 정보를 안전하게 보호하고, 여러 가지 보안 문제를 해결할 수 있는 안전한 애플리케이션 보안 구조에 대한 설계 및 구현에 대해 기술하였다. 기업의 웹 서비스는 B2B 와 B2E 로 구분되는 데, 특히 B2B 거래 시의 법적 증명력을 가지기 위한 전자 거래 법규정에 따른 정보 시스템의 보안 구성 요건을 철저히 분석하여, 시스템 구현에 적용하였다. 아울러 향후 기업의 웹 기반 애플리케이션 시스템 보안 구조의 발전방향을 살펴보면서 웹 기반 정보 시스템의 보안 환경을 검토하거나, 추진할 때 도움이 될 수 있고자 한다.

1. 서론

기업이 e-Business 로 활동 무대를 넓혀 갈 때 우선적으로 당면하는 과제는 보안이다. 이러한 e-Business 활동 상의 보안을 유지하기 위한 주요 요소들을 살펴보면, 첫 번째는 자주 거론되는 인터넷 웹 서비스 보안이고, 두 번째는 인터넷에 던져지는 전자적 기업 상거래를 보호하기 위한 전자서명 등의 보안 요소이다.

또한 e-Business 를 동적이고 실시간으로 처리하기 위해 기업 내부적인 시스템 통합과 함께 발생하는 시스템간 인터페이스 보안이나, 내부 사용자의 시스템 접근을 통제하는 보안은 아직도 허술하다. 하지만 Open Office, Mobile Office 를 지향하면서 기업의 내 외부 Network 의 구분이 물리적으로만 구분하기 어려운 상황이 되어가고 있는 것이 사실이다. 세 번째로 기업 내부 시스템의 Interface 보안과 사용자 접속 통제가 또 하나의 중요한 요소이다.

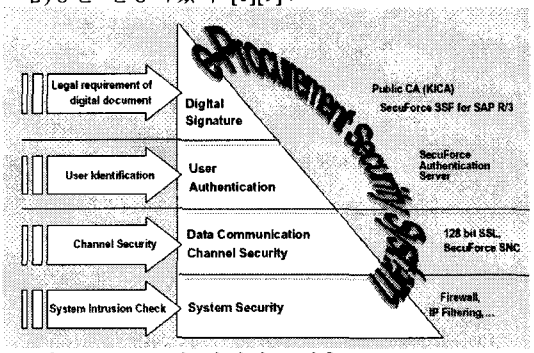
본 논문의 구현사례는 국내 선두의 통신 서비스 업체로써 내부 시스템 통합과 더불어 외부 업체들과의 e-Procurement 시스템을 인터넷 웹 기반으로 서비스를 추진하였다. 기업의 응용 애플리케이션을 웹 서비스화 할 때 갖추어야 할 여러 가지 보안 요소들을 살펴보고, 아울러 적용 시 일반 거래가 아닌 전자 거래의 법적 유효성을 증명하기 위한 법적 요구 사항에 대응되는 정보 시스템 보안 구성의 설계 및 구현에 대해서도 살펴보면서, 기업 애플리케이션의 동향에 따른 보안 환경의 발전방향에 대해 전망해 본다.

2. B2B 웹 서비스 보안 구조와 구성 사례

인터넷 기업 상거래를 위한 안전한 보안 구조는 4 가지 계층을 갖춘 피라미드 구조로 볼 수 있다. 시스

템 보안, 데이터 통신 채널 보안, 사용자 인증 보안, 법적 효력을 위한 전자 서명으로 나눌 수 있다. 아래 그림 1 과 같이 4 개의 계층 구조로 보안 계층을 나누었는 데, 이러한 계층 분류는 기업 애플리케이션의 Business 중요도와 유형에 따라 계층별로 적용 가능한 장점이 되었다.

가장 하단의 첫번째 계층은 시스템 침해 공격을 막을 수 있는 보안의 기초 요소로서 IP Filtering 기술을 기초한 Firewall, IDS(Intrusion Detect System : 침입탐지 시스템)등을 활용하였다 [1][9].



<그림 1> B2B 보안 환경의 4 계층 구조도

두 번째 계층은 Data Communication Channel 에 대한 보안으로 TCP 계층 위에 위치하는 통신 계층에서 데이터 암호화를 통해 메시지 기밀성 또는 Server 와 Client 간의 상호 인증, 메시지 무결성을 확인할 수 있다. 웹 서비스를 위해 웹 서버와 웹 브라우져 간의 대표적인 Channel Security 로는 SSL (Secure Sockets Layer) 인데, Netscape 사에서 개발되었으나 활용이 편리하고 범용적이며, 사용도 편리하여 128bit SSL 로 적용하였다 [1][4].

세 번째 계층은 사용자 신원확인을 위한 사용자 인증 계층이다.

컴퓨터 네트워크를 통한 비 대면 방식의 전자적 거래는 기존 거래 방식에서 시간적· 공간적 제약의 문제점을 해결해 주고 있으나, 신원 확인의 어려워, 중요한 거래 정보가 쉽게 노출 되어, 사용자에게 역기능을 제공할 우려가 있다.

일반적으로 웹 서버 제품의 Configuration 에서 활성화되는 SSL 의 적용은 Server 의 Certificate 만 Client 에게 전달함으로써 사용자만이 서버를 확인하는 단 방향 인증을 제공한다. 두 번째 계층의 목적인 Data Communication Channel 은 보호할 수 있지만, 권한 있는 사용자인지 확인하고 접속을 허용해야 할 지 말아야 할 지 단지 ID 와 Password 만을 가지고 판단하기엔 위험하다.

그래서 직접 대면하거나 이에 준하는 절차를 거쳐 사용자에게 전자 인증서를 발급하고 웹 서비스 접속 시 인증을 받도록 한다. 전자 인증서는 공인 인증기관에서 발행하는 공인 인증서와 기업 자체적으로 인증 서비스를 하여 발행하는 사설 인증서가 있는 데, 어떤 방식을 선택할 지는 기업의 비즈니스 환경에 맞추어 결정할 수 있지만, 정보통신부의 정책 방향에 따라 공인인증 서비스를 활용하면, 신원확인 시 대면확인의 부담을 줄이고, 신뢰성을 높일 수 있으며, 투자 비용 부담이 줄어드는 장점이 있다. 또한 네 번째 계층에서 얘기될 전자 거래의 증명력도 높일 수 있다. 아래 표 1 은 기업 입장에서 사설 인증서와 공인 인증서 사용의 차이점을 구체적으로 비교분석하였다 [8][11].

<표 1> 사설 인증 서비스와 공인 인증 서비스 비교

항목	사설 인증 서비스	공인 인증 서비스	
		법인 인증서 서비스	RA(Registry Authority) 등록기관 서비스
법적 효력	상법 적용 가능(전자거래 증명력 낮음)	전자상거래법의 효력 발생 (전자거래 증명력 높음)	전자상거래법의 효력 발생 (전자거래 증명력 높음)
인증서의 범용성	당사와의 거래에만 유효	공인 인증 기관간 상호 유효	공인 인증 기관간 상호 유효
인증 절차 편의성	편리 (FAX 및 방문으로 관련 서류 제출 후)	불편 직접 방문 (1 급 인증서), 서류 제출 이중 부담	편리 (FAX 및 방문으로 관련 서류 제출 후)
신원 확인 신뢰성	거래 상대자로써 관련 서류 검토 후 직접 발급하므로 정확함	신뢰성이 낮음. (공인 인증 기관에서 서류만으로 발급)	거래 상대자로써 관련 서류 검토 후 직접 발급하므로 정확함
거래 상대자 인증서 관리 책임	자체 인증 시스템 관리 부담	관리 부담 없음	-자체 RA 시스템 관리 부담 -발행 인증서로 타사 거래 가능하여 문제 발생 시 신원확인 책임 부담 우려
투자 비용	모든 관련 시스템 구매 및 운영 비용 부담 (약 3 억 ~ 10 억)	-법인 인증서 100,000 원/년 (거래업체의 인증서 비용을 부담할 경우: unlimited 3 천만원) -웹서버인증서 500,000 원/년	-서버 인증서 : 500,000 원/년 -웹 서버 인증서 : 500,000 원/년 -관련 시스템 구축 및 운영 비용 (약 3 억~ 10 억)

또한 전자 거래의 법적 효력을 위해 거래상대자가 법인인 경우 법인용 공인 인증서를 사용하도록 하고, 사용자 신원확인의 신뢰도가 낮은 문제점을 보완하기 위하여 사용자 등록 시 별도의 서류 제출과 대면확인 절차를 수행하도록 했다. 또한 사용자도 웹 서버가 S 사의 웹 서버임을 확인할 수 있도록 웹 서버용 공인 인증서를 적용하여 양 방향 인증이 되도록 하였다.

마지막으로 네 번째 B2B 보안 계층은 전자거래의 법적 효력을 갖출 수 있는 전자 서명(Digital Signature)이다.전자 서명이란 정당한 사용자임을 인증하고, 메시지가 위변조 되지않았음을 확인하는 무결성과 서명 사실에 대한 본인 부인 시 이를 방지할 수 있는 부인 봉쇄를 대비할 수 있다. 소인수 분해의 어려움에 기인한 RSA(Rivest-Shamir-Adleman)알고리즘을 기초로 공개키와 개인키의 조합을 이용하며, 발신자는 자신의 개인키로 서명을 암호화해서 보내고, 수신자는 발신자의 공개키로 복호화해서 발신자가 바로 그 사람임을 확인할 수 있도록 한다 [2].

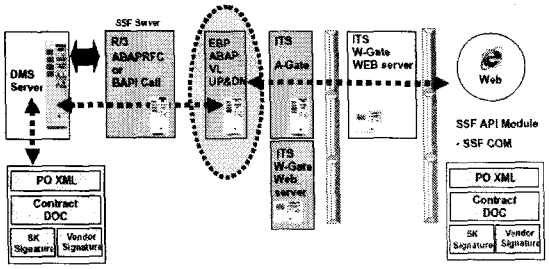
3. 전자 거래 법규에 따른 보안 요건 분석 과 적용

전자 문서와 전자 서명의 법적 효력을 갖추기 위하여, 한국의 전자 거래 관련 법 규정에 따른 보안 시스템 구성의 필요 조건들을 아래 표 2 와 같이 분석하고, 보안 시스템 구성에 적용하였다.

<표 2> 전자거래 법규에 따른 보안시스템 구성요건

구분	법 조항	보안 시스템 구성 요건
전자 서명 관련 조항	-전자거래 기본법 제 6 조 -전자서명법 제 3 조	공인 인증기관의 인증 서비스 활용한 전자서명 적용
전자 문서 보관 조항	전자거래 기본법 제 8 조	전자문서 보관 대상 -전자 문서 원본 -재현을 위한 해쉬함수용 MD(Message Digest) 보관
개인 정보 보호 조항	전자거래 기본법 제 13 조	전송과 보관과정의 안전을 위한 시스템 대책 -데이터 통신 채널 보안 -전자문서 서명 시 MD(Message Digest 보관) -정보처리과정의 시스템 무결성 -Authorization 관리
컴퓨터 등의 안전성 조항	전자거래 기본법 제 14 조	관련 시스템들의 시스템 보안 적용 -Firewall, IDS -Computer Virus 백신

e-Procurement 서비스에서의 적용 사항들을 살펴보면 다음과 같다.



<그림 2> e-Procurement 전자서명과 전자문서 보관 구조

위 그림 2 의 처리과정은 PO(Purchasing Order) 구매요청문서의 전자 서명과 전자문서 보관 과정에 대한 처리흐름을 나타내며 상세 흐름은 다음과 같다.

① 발신자는 전자서명용 법인 공인인증서로 전자서명한다.
② 전자문서를 수신한 업체는 전자문서의 서명을 확인(Verification)하고
③ 수신자는 문서 내용에 대한 확인 서명(co-Sign)을 한다
④ 발신측(Server System)은 업체의 확인 서명을 다시 확인(Verification)한다

이 과정에서 모든 PO 문서는 XML 로 처리되는 데, 전자문서의 서명 내용 (XML)과 전자문서의 표현양식(XSL)을 구분하기 위함이다. 발송자의 서명 후 수신자에게 웹 브라우저로 조회될 때 회사 로고, 송수신 날짜 등 표현 형식이 틀려서 전자문서의 무결성을 깨뜨리지 않아도 되며, 필요 없는 표현 양식까지 암호화하거나 보관해서 시간과 비용을 낭비하지 않아도 되는 여러 가지 이점이 있다.

전자 문서의 보관 시점은 발신자의 서명 직후와 수신자의 확인 서명 직후이며, 서명 후 원본과 전자 서명은 DMS(Document Management System)에 보관된다. 이 때 보관되는 전자 서명의 형태는 전자문서 원문의 해쉬 함수 처리 후 개인키의 전자서명 알고리즘 적용 결과값인 MD(Message Digest)만을 보관하는 데, 송신자와 발신자의 MD 를 쌍으로 보관한다.

그리고 이러한 PKI 공개키 기반의 전자서명은 MD 의 Size 가 작아 보관 처리가 용이할 뿐만 아니라, 법규정에 따라 장기 보관 시에도 Disk Storage 의 장소를 많이 차지하지 않는 장점이 있다 [1].

또한 기업 내부의 정보처리 과정의 시스템 무결성을 확보하고, 법인용 전자서명에의 접근을 통제하기 위하여, 시스템 내 Business Transaction 에 대한 접근권한(Authorization)관리도 중요하다. 접근권한을 가진 사용자가 ID 를 유출 또는 분실하지 않도록 로그온과 법인 인증서에 접근 시 지문 등의 생체 인식을 통하여 신원확인을 한다. 현재까지 개발된 생체 인식 기술 중 지문 인식은 비교적 적용이 용이하고 저렴하다. 다른 사람의 지문을 잘못 인식하는 타인수락오류율(FAR)은 0.005~0.00003%이고, 등록된 지문을 인식하지 못하는 본인거부 오류율(FRR)은 0.1~2.8%정도로 오류율이 낮지만 아직도 습기에 약하고 광학 센서를 이용할 경우 일반 마우스보다 커지거나, 별도의 USB 포트를 활용해야 하는 단점이 있다 [3][7].

Organization	Nationality	EER	ZeroFMR	Time(Sec.)	
				Enroll	Match
Bioscrypt Inc.	USA	0.19%	0.38%	0.11	1.97
		0.77%	1.29%	0.07	0.22
<anonymous>	?	0.33%	1.29%	2.12	1.98
		0.41%	1.44%	1.23	1.13
Suprema Inc.	Korea	0.90%*	2.69%	0.43	0.45
		2.50%	6.14%	0.54	0.63
Siemens AG	Germany	0.92%	2.29%	0.48	0.52
Neurotechnologija Ltd.	Lithuania	0.99%	3.11%	0.56	0.56
Sagem	France	1.18%	4.21%	4.05	1.65
		1.42%	4.60%	0.77	0.66

<표 3>2002 년 제 2 회 세계 지문인식 컨테스트 (FVC2002) 결과 (주요 5 개 업체)

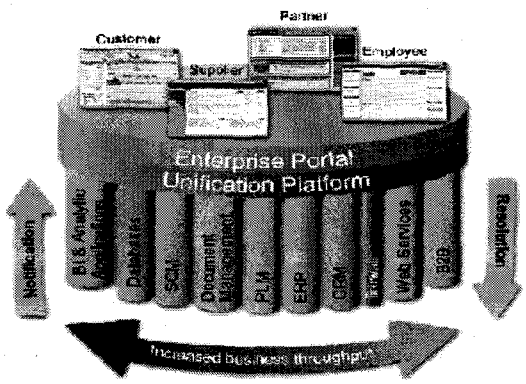
4. 기업 애플리케이션 시스템의 보안 이슈 동향

급변하는 기업의 생존환경에 따라 기업의 경쟁력을 높이는 수단으로 IT 시스템들이 우후죽순 구축되어 왔다. 90 년 대 후반 급팽창한 인터넷 앞에서도 미국 서부시대의 Gold Rush 를 연상시킬 정도로 앞 다투어 웹 사이트를 만들어 왔지만, 전자상거래나 고객 서비스를 중심으로 웹 서비스에 투자를 집중해왔다. 고객과 업체는 하나의 기업을 중심으로 제공되는 여러 가지 IT 서비스에 각각 다른 Client Program 의 설치, 로그온, 사용 방법들을 견디어 내야 하는 상황에 왔다.

2~3 년 전부터는 산재하는 다양한 정보 시스템들을 통일된 하나의 Interface 로 접근할 수 있도록 하고,사용자의 역할에 따라 활용 가능한 Transaction 들을 허용해주는 관문(Portal)형태의 웹 서비스가 생기게 되었다.이는 Yahoo, Netscape 등 상업용 검색 엔진들을 중심으로 서비스되기 시작했지만, 곧 기업들도 기업 외부의 웹 서비스에 적용하게 되었고, 최근엔 기업 내부의 정보 시스템에도 응용하는 Enterprise Portal 을 구축하려는 움직임이 활발해졌다.

또한 90 년 대 후반부터 기업 내 Business Process 를 통합하여 내부 생산성 향상을 꾀해온 기업들은 외부 서비스도 내부 IT 시스템과 통합하여 동적이고 실시간으로 처리되는 내외부 비즈니스 통합을 하고자 한다.

이러한 기업의 정보 시스템의 동향을 볼 때 Enterprise Portal 은 복잡한 Business Process 의 통합으로 복잡해진 사용자 인터페이스를 다시 단순하게 돌려주는 역할을 함과 동시에 기업 경쟁력을 높이기 위한 좀 더 힘있는 무기가 될 수 있다 [5][10].



<그림 3> Enterprise Portal 개념 구성도 [6]

그러나 또 다시 당면하게 되는 과제는 보안이다.EAI(Enterprise Application Integration) 적용으로 시스템들간에 주고받는 중요한 데이터는 중간 처리자를 거치게 될 뿐만 아니라,하나의 비즈니스 트랜잭션 서비스를 제공하기 위해서 거쳐야 할 시스템들이 많아졌다.바로 시스템간 인터페이스도 보안이 적용되어야 한다. SAP R/3 시스템의 경우 System 간 인터페이스 보호를 위하여 Data Link 를 암호화할 수 있도록 SNC(Secured Network Communication)를 지원한다. 하지만 서로 다른 보안 메커니즘을 가진 솔루션들을 같은 수준의 보호된 Channel 로 Data 를 전송하려면, 동일한 규격의 산업 표준이 적용되어야 한다.

사용자 인증도 마찬가지로 보안이 이슈가 된다.ERP, CRM 등 각각의 시스템에서 따로 관리되던 사용자 ID 와 Password 를 통합 관리하면서 하나의 사용자 ID 가 유출되면 다른 Back-end System 에 모두 접근에 허용되어 버린다. 단지 사용자 ID 를 사용자에게만 관리하도록 내버려 두기엔 야기될 수 있는 피해가 크기 때문에 좀 더 강력한 사용자 인증 관리가 필요하게 된다.

5. 결론 및 향후 방향

W3C 나 IETF 등 국제 표준화 기구에서는 소프트웨어간 통신 표준 프로토콜 SOAP(Simple Object Access Protocol), 웹 서비스 등록 레지스트리인 UDDI(Universal Description Discovery and Integration), WSDL(Web Service Description Language)등의 기술 규격에 보안 문제가 본격적으로 추진되어야 한다. IBM, MS 를 비롯한 160 개 업계 컨소시엄인 WS-I(Web Service Interoperability)에서 보안 문제를 본격적으로 보안관련 웹 서비스 기술규격을 도출한다고 하니 기대해 볼 만하다 [3].

앞으로 Enterprise Portal 과 같이 기업의 웹 서비스가 통합과 분류를 계속하면서 확장될 것이다. 이러한 보안 요소가 충분히 고려된 표준 형태의 기술 요소들을 기업 애플리케이션에 적용하고자 한다.

또한 이러한 인터넷을 바탕으로 한 보안 기술들이 보편화되어 개인과 기업들이 네트워크의 편리함을 안전하게 누릴 수 있게 되어, 교통 체증과 매연을 벗어나 재택근무 등 보다 인간적인 삶을 살 수 있게 되기를 바라는 바이다

참고문헌

[1] 이만영외 공저,전자상거래 보안 기술
[2] William Stallings, CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE
[3]http://www.etimesi.com
[4]http://news.empas.com
[5] 2002.1.17 Gene Phifer AV-14-9816 A Vertical Look at portals , http://www.gartner.com/
[6]http://service.sap.com
[7]http://www.suprema.com
[8] 朴明燮, 電子商去來와 電子支拂에 관한 小考
[9]권수갑,정보보호 기술 개념과 동향
[10]HEIDI COLLINS, Corporate Portals
[11] http://www.signgate.com