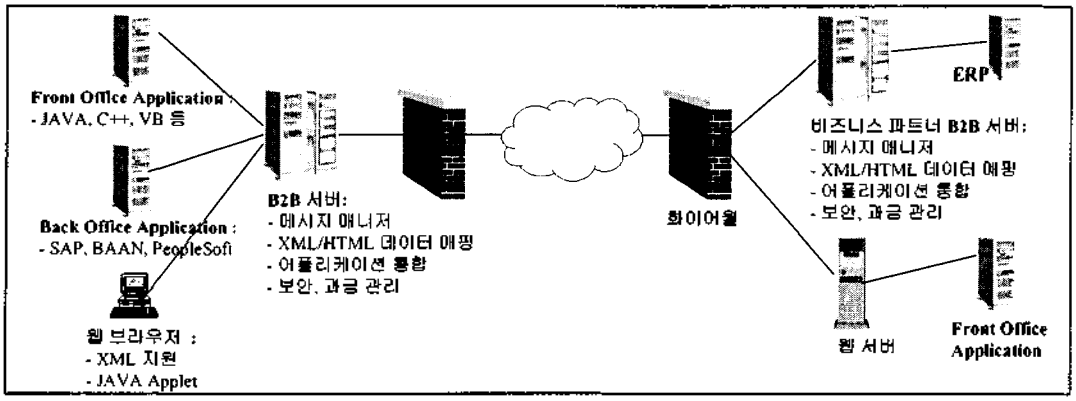
B2B 전자 비즈니스의 보안

이 현봉, 홍 성찬
한신대학교 정보통신학과

1. B2B 전자 비즈니스 구조

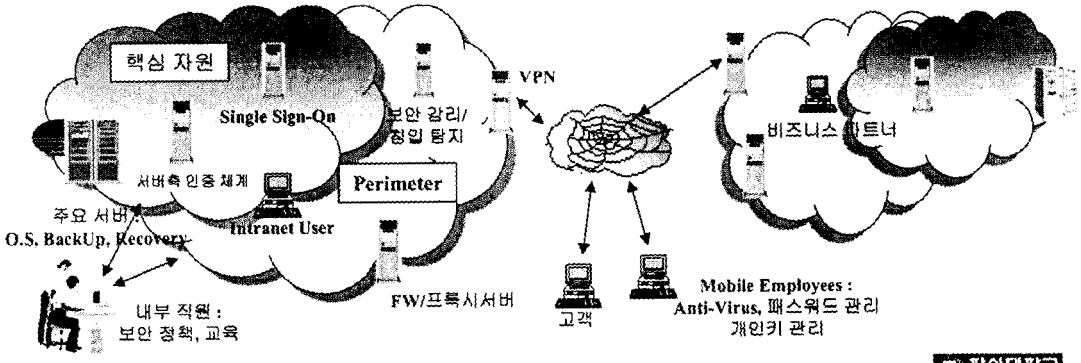
- **B2B 전자 비즈니스 유형 :**
  - EDI 와 ERP의 연계
  - 비즈니스 파트너를 위한 Online 상점 또는 도매점
- **B2B 전자 비즈니스의 보안 위협 요소 :**
  - 내부 직원, 고객, 비즈니스 파트너, 외부인
- **B2B 전자 비즈니스 기반 기술 구조 :**
  - Application 레벨에서의 통합



2. 계층적 다중 보안 체계

◆ 계층적 다중 보안 체계를 수립하여 다양한 보안 침투 가능성에 대비

- **Issue :** 시스템 통합, 표준, **Weak link** 분석/감리
  - O.S, 및 핵심 SW 보안
  - 보안 정책, 교육, 관리
  - 서버 및 호스트 보안
  - 트랜즈액션/통신 보안 : 네트워크, 세션, 어플리케이션, 파일



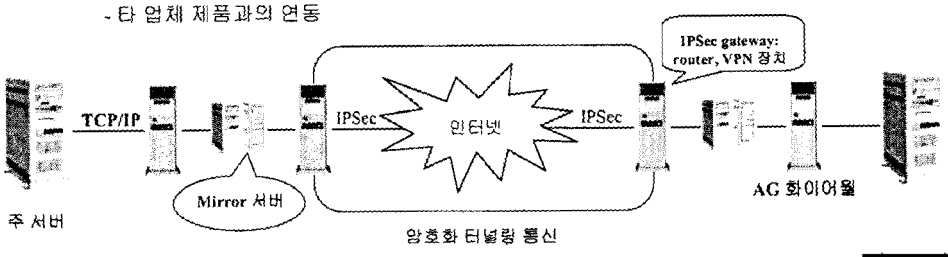
3. B2B 엑스트라넷 보안

◆ 엑스트라넷과 **B2B** 전자 거래

인증된 외부의 인트라넷으로의 접근을 허용하는 엑스트라넷은 외부 협력사의 호스트에 위치한 **B2B** 거래 관련 어플리케이션과 내부 인트라넷에 위치한 자체 **B2B** 서버를 연결

◆ 사설 개인망 (VPN) 과 엑스트라넷

- 암호와 터널링 기술을 활용하여 호스트/서버간의 보안 제공
- 이슈 :
  - 사용자 인증, 부인 거부와의 연계
  - 암호화 기법
  - 통신 프로토콜 : IPv6/IPSec, PPTP, L2F, L2TP
  - 타 업체 제품과의 연동



♦ B2B 엑스트라넷 보안의 특성

- 보안에 대한 비즈니스 쌍방의 책임
- 다수의 고객, 협력사가 채택한 다양한 정보기술 구조와의 연동에 따른 어려움
- 비즈니스 파트너간에 제기될 수 있는 다양한 요구, 책임 소재에 따른 어려움
- 계층적, 다중 보안 체계에 따른 접근 관리의 세밀함과 복잡성
- 협력사↔협력사, 협력사↔자사 간의 유동적인 사업관계에 따른 보안체계의 변화

♦ 엑스트라넷 보안 대책

- 고객과 협력사와의 협조/이해, 사안별 대립 관계를 반영한 정보 및 어플리케이션 설계
- DMZ 내에 위치한 Mirror 서버의 운영체제 및 탑재 소프트웨어에 최소한의 기능 부여
- 화이어월에 대한 제한된 신뢰
- 지속적인 교육, 감리, 모니터링, 스캐닝
- 모의 침투 시도를 통한 보안 취약점 발견 및 보완
- 공개 표준 (IPSec, X.509) 과 강력한 암호기법을 채택한 솔루션 선정
- 침입을 대비한 정책 수립
- 협력사와의 협조

한신대학교

4. XML과 디지털 서명

♦ Extensible Markup Language

- Tag (" ", " ") 의 의미를 다양하게 정의
- 스프레드 시트, 주문서, 송장, 재무 재표와 같은 구조적인 데이터를 정의하는 데 적합
- Xlink, CSS, XSL, DOM, RDF, Namespace 등의 표준과 기술을 포함
- License-free, 플랫폼 독립적이며 인터넷 컴유니티의 지원
- 인터넷 B2B 전자 거래 기반 기술로 적합

♦ W3C XML 디지털 서명 Working Draft (1999, 10, 14)

- XML 내용 (Xlink로 연결되는 Web 자원, XML의 해시 등)의 해시를 단방향 변환 함수의 키로 서명
- XML-서명은 XML로 구성된 어떠한 어플리케이션도 지원
- XML-서명의 데이터 구조는 RDF 데이터 모델에 기초해야 함
- XML-서명은 XML 문서 전체 또는 일부에 효력을 발생할 수 있음
- 여러 개의 키, 내용 변환 기술, 그리고 (해시, 암호화)알고리즘을 이용하여 하나의 웹 자원에 대하여 다수의 디지털 서명을 할 수 있어야 함

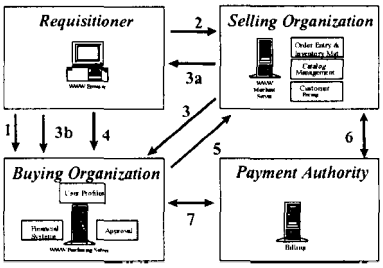
한신대학교

5. Open Buying on the Internet (OBI)

- ◆ 공개적, 안전하며 유연한 표준으로 **B2B** 인터넷 상거래 지원
  - **1999 V2.0 (소액의 대량 거래), XML** 지원 표준 미비
- ◆ **OBI** 보안 관련 표준
  - **OBI** 객체와 디지털 서명, **OBI** 객체의 안정된 전송, 인증 모델, 디지털 인증서 관리

Purpose	Standard	Existing Examples
Content Display	Evolving standards for Web browsers (currently based on HTTP and HTML) as specified by the W3C	Netscape Navigator V3.0 or later, Microsoft Internet Explorer V3.0 or later
Order Requests and OBI Orders	X12 850 EDI standard	OBI/2.0 order format specification (defined by the OBI Consortium)
Order Transmission	HTTP 1.0 using SSL	HTTP servers available from many vendors including Netscape, Microsoft, Oracle
Secure Internet Communication	SSL V3	SSL supported by many vendors including Netscape, Microsoft, Oracle
Cryptography	SSL V3 API Public Key Cryptography Standards (PKCS)	Netscape SSL API RSA BSAFE Microsoft CryptoAPI
Public Key Certificates & Certificate Authorities	X.509 V3 certificates	GTE CyberTrust Verisign

• **OBI** 모델



1) 구매 요청자 (requisitioner)가 자체 (Buying Organization) 구매 서버를 경유하여 판매자 (Selling Organization)의 머천트 서버에 있는 상품을 선택한다

2) 머천트 서버가 구매자의 디지털 인증서를 이용하여 인증 작업을 한다

3) 구매자의 장바구니와 신원을 담은 주문요청서 (EDI 호환) 와 디지털 서명을 OBI 객체로 포장하여 직접 구매 서버로 전송하거나 또는 구매자를 경유하여 (3a→ 3b) 보낸다 (HTTP, SSL 이용). 구매 서버는 수신한 OBI 객체의 서명을 검증하고 주문요청서를 추출하여 내부 결재 처리를 준비한다.

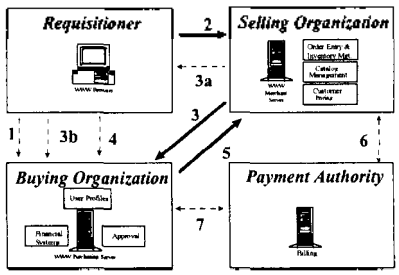
4) 기타 관리 정보 (확인, 변경, 결재 조건)를 구매 관련 인원으로부터 얻는다

5) 결재를 득한 구매요청서를 OBI 구매서로 변환하고 디지털 서명을 부착하여 OBI 객체로 포장하여 안전하게 (SSL) 판매자의 머천트 서버로 전송한다

6) 판매자는 지불 기관 (Payment Organization)에서 구매자의 신용 검증, 지불 조건 등을 처리한 후 상품 배송 준비를 한다

7) 지불 기관이 송장을 전송하고 대금 지불을 받는다

• **OBI** 거래자간 인증



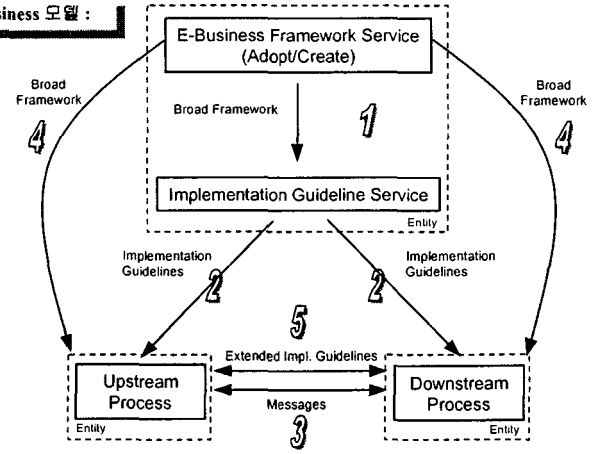
◆ OBI의 구매 처리 과정에서 거래 당사자간 인증이 다음 3 지점에서 발생한다.

- 구매자가 머천트 서버의 카타로그 정보에 접속할 때 디지털 인증서를 첨부하여 머천트 서버가 구매자의 신분을 확인 (2)
- 판매자의 머천트 서버가 구매자의 장바구니와 신원을 담은 주문요청서와 디지털 서명을 OBI 객체로 포장하여 구매 서버로 전송할 때 (3)
- 구매 서버가 결재를 득한 구매요청서를 OBI 구매서로 변환하고 디지털 서명을 부착하여 OBI 객체로 포장하여 머천트 서버로 전송할 때 (5)

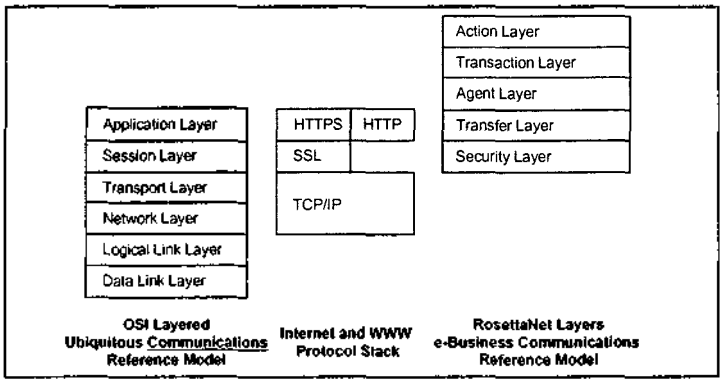
6. RosettaNet

- ♦ 공급망 (Supply Chain) 에 관여하는 비즈니스 파트너간에 공개적, 안정되며 유연한 전자거래 표준 지원
- ♦ OBI 표준을 참고하여 통신 프로토콜, XML 지원, 에이젠트 등에 대한 구체적 언급

• RosettaNet e-Business 모델 :



• ISO/OSI, 인터넷과 RosettaNet 통신 프로토콜 비교



• RosettaNet의 보안 : OBI 보안 표준과 유사
- 디지털 서명 기술 표준 : RSA Data Security 의 PKCS #7
- 안정된 인터넷 통신 : Secure Socket Layer (SSL) v.3
- 공개 키 인증서 : X.509 V3
- PKI 및 Root 인증서 : Root 인증서는 공개적이며 안정적인 방법으로 분배 (Web browser에 내장)

7. 디지털 영수증과 B2B 전자 비즈니스

♦ 기업의 사활이 걸린 기업간 극히 중요한 거래 사실에 관한 증명 필요

♦ 디지털 서명, PKI, CA, VPN, XML-EDI 등의 보안 인증 기술 및 기구

♦ 통신 또는 거래 사실에 대한 증명 :
- 증거 생성
- 증거 전송
- 증거 검증
- 증거 보관

← - CA Timestamp
- 인증서 추적 기능
- 영수증 추적 기능

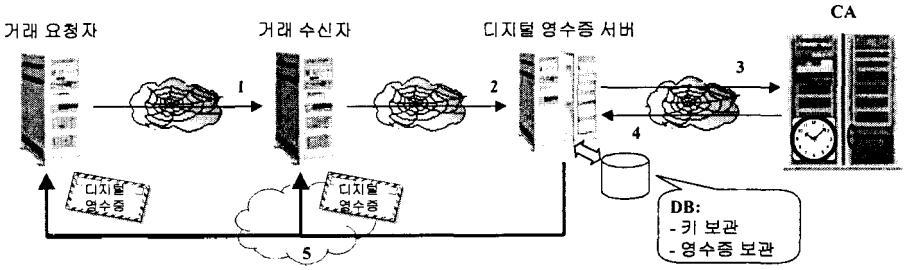
♦ 통신/거래 수신자의 보호 :

분쟁 가능성	증거
- 누가 이 통신을 보내었는 지	신원 검증 장치
- 언제 이 통신을 보내었는 지	출처의 Timestamp
- 전송 중의 내용 변조	내용 보증

♦ 통신/거래 송신자의 보호 :

분쟁 가능성	증거
- 이 통신이 잘 도착하였는 지	통신 사실 검증
- 언제 이 통신이 도착하였는 지	도착 Timestamp
- 전송 중의 내용 변조	내용 보증

♦ 디지털 영수증 모델



1) 대금 지불 & 영수증 요청
2) 디지털 영수증 서버에게 영수증 요청
3) 모든 통신 내용에 대한 인증 요청
4) 모든 통신 내용에 대하여 Timestamp, 암호화/서명된 영수증 발부
5) 거래 요청자와 거래 수신자에게 디지털 영수증 발부 & 관련 키 및 영수증 사본 보관

8. 향후 전망

- **SET**의 광범위한 보급은 **OBI**와 **RosettaNet**의 경우에서와 같이 **PKI** 수립이 전제
- 보안 장비/서비스 업체간의 기업 합병/인수와 업체들의 공개 표준 채택으로 보안 솔루션 구성이 용이해 질 것임
- **ICSA** 와 같은 기관의 등장으로 보안 솔루션에 대한 정확한 평가가 용이해 지고 있음
- 최근 들어 **Open PGP** 가 다시 힘을 얻고 있음
- **IETF**가 지원하는 **IPSec** 와 **PKIX**가 널리 보급됨
- 어플리케이션 레벨에서 **UDP**의 화이어월 통과를 다루는 **IETF**의 **Authenticated Firewall Traversal (AFT)** 과 같은 서비스 필요
- **XML+JAVA**를 기반으로 하는 보안 제품의 등장이 활발해 질 것임