'99 전자거래(CALS/EC)종합학술대회 발표논문

웹기반 은행업무를 위한 보안시스템 구축방안

A Practical Guideline for Implementation of the Web Banking Security Systems

김 상 균
산업정보시스템연구실
연세대학교 인지과학 산업시스템공학전공
saviour@iis.yonsei.ac.kr

임 춘 성
산업정보시스템연구실
연세대학교 기계전자공학부 정보산업전공
leem@yonsei.ac.kr

목 차

■ 연구배경 및 필요성
■ 연구목적 및 범위
■ 웹기반 은행업무
■ 보안 목표 수립
■ 보안 위협요소 분석
■ 보안 메커니즘 설계
■ 보안 메커니즘 검증
■ 패키지기반의 보안 시스템 구성
■ 결론
■ 참고문헌

연구배경 및 필요성

ν 연구배경
- 인터넷 사용자 증대 및 웹기반 서비스 확산**[Report,1998]**
- 웹기반 은행업무의 등장**[Arie,1998]**[임춘성,**1998]**
- 인터넷 기반 보안 사고의 증대**[임차식,1998]**
- 인터넷 기반 시스템 침해 기법의 다양화**[FIST,1998]**

ν 연구필요성
- 웹기반 은행 업무의 보안 위협에 대한 분석 필요
- 보안 위협요소에 대한 보안 모델 수립 필요
- 현존하는 보안 패키지 시스템의 웹기반 은행업무 적용방안 필요

연구목적 및 범위

■ 연구목적

λ 웹기반 은행업무의 보안 모델을 수립하고, 이를 바탕으로 현존하는 패키지 시스템을 통하여 구축가능한 시스템모델을 제시하여, 웹기반 은행업무의 활성화와 서비스 다각화에 기여함을 본 연구의 목적으로 한다.

■ 연구범위

λ 웹기반 은행업무 시스템 분석

λ 웹기반 은행업무의 보안 목표, 위협요소 분석

λ 웹기반 은행업무를 위한 보안 모델 수립

λ 패키지 시스템을 통한 보안모델의 실현화 방안 수립

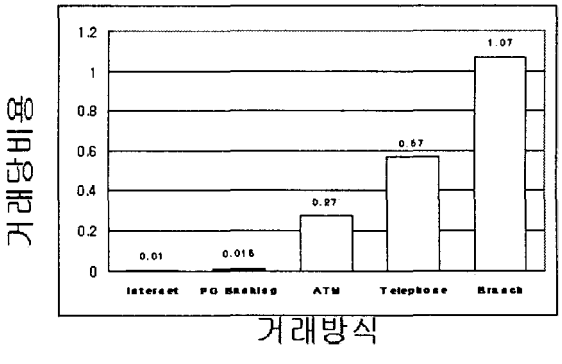
웹기반 은행업무- 주요업무

[Gloria,1998]

Banking Services Provided on the Internet	
Bill Payment (BP)	계좌관리
Account Balance (ACB)	
Funds Transfer (FT)	
Cheque Issuance (CHQ)	
Online Credit Card Pre-authorization (OCC)	
Online Mortgage Pre-authorization (OLM)	
Online Loan Pre-authorization (OLL)	
Downloadable Financial Tools, Forms and Information (DFT)	정보조회
Electronic Commerce Capability (EC)	부가서비스
Products and Services Information (P&S)	
Corporate Information (CI)	
Investment Information and Statistics (Stat)	
E-mail Capability (Email)	
General Information (GI)	

웹기반 은행업무- 기대효과

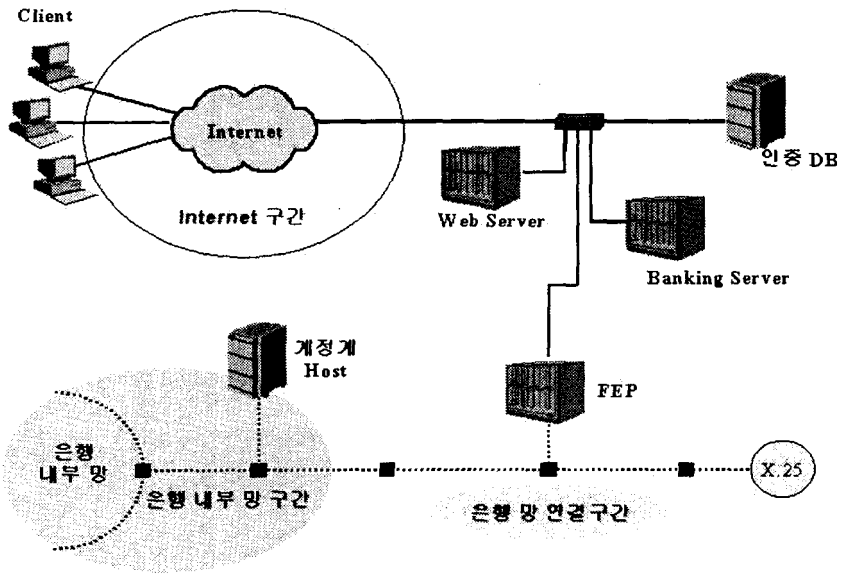
- 전자 네트워크를 통한 고객저변의 확대[John,1999]
- 고객정보의 축적과 그에 따른 마케팅 전개[Maurice,1998]
- 즉시성 및 항시성 제공으로 고객만족도 향상[David,1999]
- 새로운 사업분야 진출가능[임춘성,1998]
- 업무집약 및 합리화에 의한 경비절감[David,1999]



웹기반 은행업무 - 시스템구성(1)

- 시스템 구성요소[Arie,1998][임춘성,1998]
  - λ Client(고객)
  - λ Web Server(은행 웹서버)
  - λ CA(은행의 고객 인증 시스템, 인증 DB)
  - λ Banking Server(웹기반 서비스 제공)
  - λ FEP(Front End Processor : 기존 은행망과 연계)

웹기반 은행업무 - 시스템구성(2)



보안목표 수립

- ST-1:사용자에 대한 식별 및 인증을 통하여 허가되지 않은 사용자의 불법적 접속을 차단한다.
- ST-2:인터넷 구간을 통하여 고객과 은행과의 통신이 수행되는 동안, 통신내역에 대한 도청 및 위변조를 차단한다.
- ST-3:웹기반 은행 업무가 항상 정상적인 속도를 유지하도록 한다.
- ST-4:웹서버, 인증서버 및 뱅킹서버는 허가된 관리자에 의하여 정보와 기능을 변경할 수 있도록 한다.
- ST-5:뱅킹서버에 문제가 생긴 경우에도, 은행 내부망으로의 침투는 철저히 차단한다.
- ST-6:고객의 신용 및 계좌관련 정보가 외부로 유출되지 않도록 한다.

* ST : Security Target

보안위협요소 분석

- SV-1:인증되지 않은 사용자가 웹기반 은행업무 시스템에 접속하는 위협
- SV-2:권한없는 사용자가 인증된 사용자의 인증정보를 위조하여 불법적 접근을 시도하는 위협
- SV-3:인터넷 송수신로 상에서 고객과 은행과의 통신정보가 도청되거나 위변조되는 위협
- SV-4:인증된 고객이 자신이 사용한 거래내역을 부인하는 위협
- SV-5:은행업무에 차질을 줄 목적으로 외부에서 웹기반 은행업무 시스템의 속도를 저하시키거나, 접속을 못하도록 방해하는 위협
- SV-6:권한없는 자가 인증서버의 정보를 위변조하거나, 침투 프로그램을 설치하는 위협
- SV-7:권한없는 자가 웹서버의 정보를 위변조하거나, 침투 프로그램을 설치하는 위협
- SV-8:권한없는 자가 뱅킹서버를 무력화 시키거나, 기능을 변조하는 위협
- SV-9:권한없는 자가 은행내부망으로 침투하는 위협
- SV-10:은행내부 업무관련 정보 및 고객정보를 외부로 송출하는 위협

* SV : Security Vulnerbility

보안메커니즘 설계

- **SM-1:**고객과 은행과의 통신내역을 암호화시켜 제3자의 도청을 막는다.
- **SM-2:**고객에 대하여 일회용 암호를 사용한 인증 및 브라우저 인증을 통하여 불법적 사용자의 접속을 막는다.
- **SM-3:**웹서버와 인증 및 뱅킹서버간에 차단시스템을 설치하여 웹서버에 설정된 은행업무용 접속만을 허용하도록 한다.
- **SM-4:**뱅킹서버와 은행내부망을 차단하여 뱅킹서버에 문제발생시 내부망이 침해되지 않도록 한다.
- **SM-5:**웹서버, 뱅킹서버, 인증서버 및 차단시스템의 관리기능을 위한 접근은 암호화 인증 및 접근제어를 통하여 인가된 관리자만이 접근가능하도록 한다.
- **SM-6:**웹기반 은행업무를 위한 전산시스템에 대하여 지속적으로 취약성검사를 하여 보안상의 위협요소를 사전에 탐지하고 조취한다.
- **SM-7:**침입탐지 기능을 통하여 불법적 접근 및 공격 내역을 탐지하고 실시간으로 이에 대응하도록 한다.
- **SM-8:**외부로 송출되는 자료의 컨텐츠를 검사하여, 고객 신용 및 계좌관련 정보가 외부로 누출되는 것을 차단한다.
- **SM-9:**악의적인 프로그램이 웹기반 은행업무를 위한 전산시스템에 탑재되는 것을 방지하기 위하여 실시간으로 바이러스에 대한 검색 및 치료를 수행한다.

* SM : Security Mechanism

보안메커니즘 검증

■ 보안메커니즘을 통한 보안목표 만족

	SM-1	SM-2	SM-3	SM-4	SM-5	SM-6	SM-7	SM-8	SM-9	
ST-1		▨	▨			▨	▨			4
ST-2	▨					▨				2
ST-3		▨				▨	▨		▨	4
ST-4			▨		▨	▨	▨		▨	5
ST-5				▨		▨	▨			3
ST-6								▨		1
	1	2	2	1	1	5	4	1	2	

보안메커니즘 검증

■ 보안메커니즘을 통한 보안위협요소 대응

	SM-1	SM-2	SM-3	SM-4	SM-5	SM-6	SM-7	SM-8	SM-9	
SV-1		▨								1
SV-2		▨				▨	▨			3
SV-3	▨					▨				2
SV-4		▨	▨							2
SV-5						▨	▨		▨	3
SV-6			▨		▨	▨	▨		▨	5
SV-7					▨	▨	▨		▨	4
SV-8			▨		▨	▨	▨		▨	5
SV-9			▨	▨			▨			3
SV-10								▨		1
	1	3	4	1	3	6	6	1	4	

패키지기반의 보안시스템 구성

- 시스템 통합 관점에서의 보안 시스템 구성
  - 관련된 보안 패키지의 선별
  - 보안패키지간의 유기적 연계를 통한 보안메커니즘 구현
- 보안패키지의 선별
  - 침입차단시스템
  - 침입탐지시스템
  - 바이러스탐지 및 제거 시스템
  - 취약성 분석 도구
  - 사용자 인증시스템
    - ◆Client - 고객
    - ◆Server - 은행
  - 암호화 통신 시스템

패키지기반의 보안시스템 구성

■ 보안패키지별 주요기능 – 침입차단 시스템

[Rolf,1997][Christoph,1997]

- λ **Application Gateway**
- λ **Packet Filtering**
- λ 파일 무결성 검증
- λ 관리자에 대한 암호화 인증
- λ 사용자 인증
- λ 접속내역 기록 및 검색, 조회

패키지기반의 보안시스템 구성

■ 보안패키지별 주요기능 – 침입탐지시스템

[Rebecca,1999][김상균,1998]

- λ 관리자에 대한 암호화 인증
- λ 시스템에 대한 보안관리
- λ 실시간 네트워크 감시
- λ 실시간 침입탐지 및 경보
- λ 네트워크 사용 감사기록
- λ 감사기록의 검색 및 조회, 보고서 출력

패키지기반의 보안시스템 구성

- ν 보안패키지별 주요기능 – 바이러스탐지 및 치료 도구
  - 네트웍 기반 바이러스 탐색 및 치료
  - 바이러스 정보DB유지 및 제품제공사로 부터의 주기적 갱신
  - 바이러스 탐색 및 치료시스템에 대한 보안성 확보

패키지기반의 보안시스템 구성

■ 보안패키지별 주요기능 – 취약성분석도구

[김상균,1998][박성득,1998]

- λ 취약성 분석 DB 구축
- λ DB를 기반으로 시스템에 대한 정기적 점검
- λ 서버, 호스트의 설정내역에 대한 취약성 분석
- λ 관리자, 사용자 암호의 재설정 요구
- λ 점검된 취약성에 대한 보완 방안 제시
- λ DB의 지속적 갱신

패키지기반의 보안시스템 구성

■ 보안패키지별 주요기능 – 사용자인증시스템

[Sharon,1999]

- λ 특정 서비스를 이용하려는 사용자들을 구분하기 위한 전자적인 신분증(인증서)을 발급하는 시스템
- λ **Browser & Server**를 위한 **Netscape/Internet Explorer** 인증서 발급
- λ 표준 **X.509** 기술 채택 **(X.509 Version 3** 사용**)**
- λ 인증용 **RSA Key** 길이 **(512 bit ~ 4096 bit)**
- λ **OTP(One Time Password)**기능의 인증 프로그램과 연계

목 차

■ 연구배경 및 필요성
■ 연구목적 및 범위
■ 웹기반 은행업무
■ 보안 목표 수립
■ 보안 위협요소 분석
■ 보안 메커니즘 설계
■ 보안 메커니즘 검증
■ 패키지기반의 보안 시스템 구성
■ 결론
■ 참고문헌

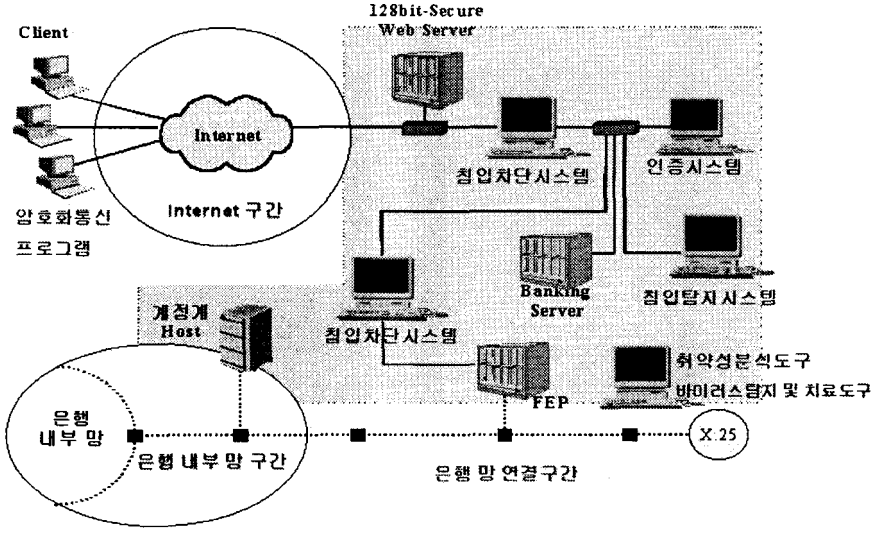
패키지기반의 보안시스템 구성

■ 보안패키지와 보안메커니즘과의 상관분석

	침입차단 시스템	침입탐지 시스템	바이러스 탐지 및 치료 도구	취약성 분석도구	사용자 인증 시스템	암호화 통신 시스템
SM-1						▨
SM-2					▨	
SM-3	▨					
SM-4	▨					
SM-5	▨					
SM-6				▨		
SM-7		▨				
SM-8		▨				
SM-9			▨			

패키지기반의 보안시스템 구성

■ 보안패키지를 통한 시스템 구성도



결론

- 연구결론
  - 웹기반 은행업무를 통하여 은행은 운영 및 서비스 경쟁력을 향상할 수 있다.
  - 현존하는 웹기반 은행업무 모델은 많은 보안상의 취약성을 가지고 있다.
  - 본 논문에서 제시한 패키지 기반 보안시스템의 구축을 통하여 웹기반 은행업무의 보안성을 확보할 수 있다.
- 향후 연구 과제
  - 패키지의 통합화를 통한 시스템의 보안성 강화방안 연구
  - 패키지기반 은행업무 보안 시스템의 실증적효과성 검증
  - 보안패키지 도입시 전략수립 및 의사결정 지원을 위한 지원시스템 개발
  - 보안 시스템의 운영 및 감리에 대한 연구
  - 은행내부 업무프로세스에 대한 보안성 강화방안 연구

참고문헌

[Arie,1998] Arie Segev, Jaana Porra and Malu Roldan, "Internet Security and The Case of Bank of America", *Communications of the ACM*, Vol. 41, No. 10, October 1998.

[Christoph,1997] Christoph L. Schuba and Eugene H. Spafford, "A Reference Model for Firewall Technology", *IEEE*, 1997.

[David,1999] David Henry, "The Emerging Digital Economy II", U.S. Department of Commerce, June 1999.

[FIST,1998] FIST(Front-line Information Security Team), "Techniques Adopted By 'System Crackers' When Attempting To Break Into Corporate or Sensitive Private Networks", *Network Security Solutions Ltd.*, December 1998.

[Gloria,1998] Gloria Yan and Joseph C. Paradi, "Internet – The Future Delivery Channel for Banking Services?", *31st Annual Hawaii International Conference on System Sciences*, 1998.

[John,1998] John Skipper, "Electronic Banking and Payments", *The Institution of Electrical Engineers*, 1998.

[Maurice,1998] Maurice Mulvenna, "Data-Driven Marketing", *Electronic Markets*, Vol. 8, No. 3, 1998.

[Rebecca,1999] Rebecca Bace, "An Introduction to Intrusion Detection and Assessment", *ICSA*, 1999.

[Report,1998] "U.S. Government Working Group on Electronic Commerce First Annual Report",Novermber 1998.

[Rolf,1997] Rolf Oppliger, "Internet Security : Firewalls and Bey", *Communications of the ACM*, Vol. 40, No. 5, May 1997.

[Sharon,1997] Sharon Boeyen, "Certificate Policy and Certification Practice Statements", *Entrust Technologies*, 1997.

[김상균,1998] 김상균, "SET기반 전자상거래를 위한 보안 시스템의 설계 및 운영에 관한 연구", *연세대학교 산업공학 석사학위논문*, 1998. 6.

[박성득,1998] 박성득, "위험분석 방법론 및 자동화 도구 기술이전 교육교재", *한국전산원*, 1998. 9.

[임차식,1998] 임차식외 6인, "정보화 역기능 현황, 분석 및 대응방안 연구", *한국정보보호센터*, 1998. 1.

[임춘성,1998] 임춘성, "전자상거래", *북풀러스*, 1998. 3.