우리나라 전자지불시스템 현황 분석을 통한 안전한 전자지불시스템의 연구

송 용 욱* · 이 재 규** · 황 재 훈*

Development of a Secure Electronic Payment System based on the Analysis of Current Korean Electronic Payment Systems

Yong Uk Song* · Jae Kyu Lee** · Jaehoon Whang*

Abstract

As Electronic Commerce is popularized, crimes related to Electronic Commerce are also increasing. Electronic shopping malls and payment gateways focus their attention on network security of payment information or the sizes of encryption keys. In real world, however, the payment-related crimes in electronic shopping malls are not based on the security hole of encryption mechanism of the payment systems, but on the customers carelessness or the insecurity of server systems of merchants or financial institutes. So, this research analyzes the structure of current electronic payment systems, investigates the payment-related crimes, addresses the structural problems of the Korean electronic payment systems, and suggests an alternative general architecture for secure payment systems by incorporating the concept of separation of order information and payment information.

Keywords : Electronic Commerce, Payment System, Authentication, Security

※ 본 논문은 2000년도 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2000-003-C00263).
* 연세대학교 원주캠퍼스 경영·정보학부
** 한국과학기술원 테크노경영대학원

1. 서 론

우리나라 전자상거래가 연 200%가 넘는 고도의 성장기를 지나 이제 안정화 단계에 들어서면서 전자상거래는 점차 우리 생활의 일부가 되어 가고 있다. 그러나, 이것은 동시에 전자상거래 관련 범죄의 대중화 및 그 발생 빈도의 증가도 함께 의미한다. 본 논문에서는 일반 소비자와 관계된 B2C 전자상거래 관련 범죄 중에서 전자지불시스템 관련 범죄에 초점을 맞추어 그 보안 현황을 점검하고, 그 문제점 및 해결방안을 모색하고자 한다.

현재 우리나라 전자쇼핑몰 또는 지불대행업체들이 전자지불시스템 보안과 관련하여 강조하는 것은 지불 정보의 네트워크 보안 및 그 암호화 키의 크기이다. 네트워크 보안을 위하여 대부분의 전자지불시스템들은 키 크기 128Bit의 SSL 보안 기법을 사용하며, 그 점을 마케팅 측면에서도 강조하고 있다. 그렇지만, 실제로 일어나고 있는 전자쇼핑몰의 지불사고는 "부당대금 청구", 즉, "신용카드 도용에 의한 예상치 않은 대금 청구"의 형태이며, 그러한 사고들의 경위를 살펴보면 고객의 카드정보 및 유효기간 등의 민감한 정보가 지불정보시스템의 암호화 보안 허점을 통하여 유출되기 보다는 고객의 부주의나 쇼핑몰, 지불대행업체 또는 금융기관의 시스템 보안 허점을 통하여 유출된 사례들이 전부를 차지하고 있다. 따라서, 본 연구에서는 현재의 우리나라 전자지불시스템의 구조 분석을 통하여 민감한 지불 정보의 유출 가능 통로를 파악하고, 현재까지의 전자지불시스템들의 사고사례를 조사하여 실제로 사고가 빈발하고 있는 지불 정보 유출 통로를 찾아냄으로써 그 문제점을 파악하고, 나아가 이러한 문제점을 해결할 수 있는 전자지불시스템 보안 구조를 제시하고자 한다.

이를 위하여 본 논문의 2절에서 전자지불시스템 관련 문헌들을 살펴보고 현재 우리나라에서 가장 많이 쓰이고 있는 SSL 기반 신용카드 전자지불시스템을 알아보면서 그 연구 현황과 한계점들을 살펴보고, 3절에서 각종 사고 사례, 관련 통계 및 전자상거래 관련 기관과의 인터뷰를 바탕으로 현존 전자지불시스템 보안 취약점을 분석함으로써 현 전자지불시스템의 문제점을 파악한다. 그리고, 4절에서 문제점에 대한 이해를 바탕으로 그것을 해결할 수 있는 전자지불시스템 구조를 제시하고, 5절에서는 제시된 전자지불시스템 구조의 장단점에 대하여 토의한 후, 6절에서 결론을 맺도록 하겠다.

2. 관련 연구

2.1 전자지불시스템 관련 연구

전자지불시스템과 관련된 연구로는 전자지불시스템 분류에 관한 연구, 지불시스템간 상호운영성에 관한 연구, 지불시스템의 요건 및 비교연구, 전자지불시스템 현황에 관한 연구, 전자지불시스템 프로토콜과 모형에 관한 연구 등이 이루어져 왔다.

전자지불시스템 분류와 관련하여 Kalakota와 Whinston[1996]은 전자지불시스템을 크게 토큰기반 지불시스템, 신용카드기반 지불시스템으로 분류하였고, Crede[1996]는 지불방식과 시스템의 보안 등에 근거하여 전자현금시스템, 매개적 지불시스템, 신용카드 방식 시스템, 스마트카드 방식 시스템의 네 가지 형태로 분류하였으며, 김종률[1996]은 전자지불시스템을 화폐가치의 정보를 저장하는데 이용되는 수단에 따라 네트워크형 전자지불시스템과 가치저장형 전자지불시스템으로 분류하였다. 문종진[1996]은 결제방법 또는 사용방법상의 차이에 근거하여 가치저장형, 지불지시형, 전송형 등으로 구분하였고, 이재

규[1996]는 온라인지불형, IC 카드형, 네트워크형으로 구분하였으며, 제일금융연구원[1997]은 전자화폐를 결제수단에 따라 선불카드형, 신용카드형, 수표형, 현금형 전자화폐로 분류하였다[김창수, 홍일유, 1998]. 또한, Asokan과 Janson [1996]은 지불 거래에서 지불인과 수취인이 직접 통신하는지 또는 지불인이나 수취인 중 어느 한 당사자만이 지불시스템에 개입하는지 여부, 거래 시점과 지불 시점과의 관계, 거래 시 지불인과 수취인의 제 3자를 통한 연결 여부, 익명성의 보장 수준 등에 따라 전자지불시스템을 분류하였다[주재훈, 1999]. 현재는 전자지불시스템을 신용카드, 전자수표, 계좌이체, 전자현금, 가상계좌 등 지불수단별로 분류[이재규 등, 2002]하는 것이 일반적이며, 또한 지불수단별 분류를 바탕으로 전자지불시스템 통계[통계청, 2003] 등도 발표되고 있다.

다양한 전자지불 프로토콜과 표준이 개발됨에 따라 지불시스템 간의 상호운영성에 대한 연구도 진행되어 왔다. W3C와 CommerceNet에서는 거래자가 다양한 지불수단을 편리하게 선택하여 이용할 수 있도록 지원해주는 JEPI (Joint Electronic Payment Initiative) 프로젝트를 수행하였다[Chung and Dardailler, 1997]. 그 외에도 다양한 전자화폐 간의 호환성의 문제를 해결하기 위하여 IBM의 연구[Abad-Peiro et al., 1996], 스탠포드 대학의 Interpay 연구 [Cousins et al., 1995] 등이 수행되었다[주재훈, 1999].

지불시스템의 요건 및 여러 가지 지불시스템에 대한 비교 연구로서는 전자지불시스템의 비교분석을 위한 프레임웍을 제시한 홍일유, 김창수, 편완주[1997] 및 김창수, 홍일유[1998]의 연구, 퍼스트 버츄얼, 이캐시, 밀리센트, 몬덱스의 특성을 상호 비교한 Stalder[1997]의 연구, 전자화폐 시스템을 분석할 때 고려하여야 할 주요 요소를 분류한 Kienzle and Perrig[1996]의 연구, NII(National Information Infrastructure)를 이용하는 전자지불 시스템에서 고려되어야 할 특성을 제시한 Cross-Industry Working Team [1996]의 연구, 전자지불시스템의 기본적 서비스를 제시한 Medvinsky와 Neuman[1993]의 연구, 전자상거래에 대한 판매자 및 구매자의 요구사항을 제시한 Pays와 Comarmond[1996]의 연구, 신용카드 기반의 지불시스템을 이용하는 구매자, 판매자, 금융기관에서의 요구 사항을 제시한 Elgamal[1995]의 연구, 전자화폐의 기본 요건으로서 부정방지 능력, 프라이버시 보호와 익명성, 오프라인 능력 등을 제시한 Brands [1995]의 연구, 화폐의 일반적인 특성을 분석하고 익명성과 프라이버시 보호 관점에서 일반 화폐, 이캐시(전자화폐), 넷빌(전자수표)을 비교하여 거래 관련자들에게 노출되는 정보를 분석한 Camp, Sirbu, Tygar[1996]의 연구 등이 있다[주재훈, 1999]. 또한, 주재훈[1999]은 전자지불 시스템의 수용성 또는 범용성에 영향을 주는 안전성, 보안성, 효율성, 편리성의 4가지 차원에서 전자지불시스템의 주요 성공요인을 분석하였다.

전자지불시스템 현황과 관련하여 오형근, 이임영[1999]은 전자화폐 시스템 개발 동향에 대하여 연구하였고, 김종우, 송주석[2000]은 전자 지불 프로토콜 표준화 동향에 대하여 연구하였으며, 임신영, 조현규, 함호상, 김태윤[2000]은 전자지불 기술에 대하여 연구한 바 있다.

전자상거래를 위한 전자지불시스템 프로토콜과 모형에 관한 다양한 연구와 프로젝트 [Bellare, 1995 ; Brands, 1995 ; Brahm and Turban, 1996 ; DigiCash, 1996 ; CyberCash, 1996 ; Clifford and Ts'o, 1994 ; Master Card and Visa, 1997 ; Visa, 2001 ; 송용욱, 이재규, 1999 ; 김은영, 조동섭, 2000]도 진행되어 왔다[주재훈, 1999]. 이들 중 일부는 실험적 연구 수준에서 그친 것도 있으나, DigiCash, CyberCash, SET[Master Card

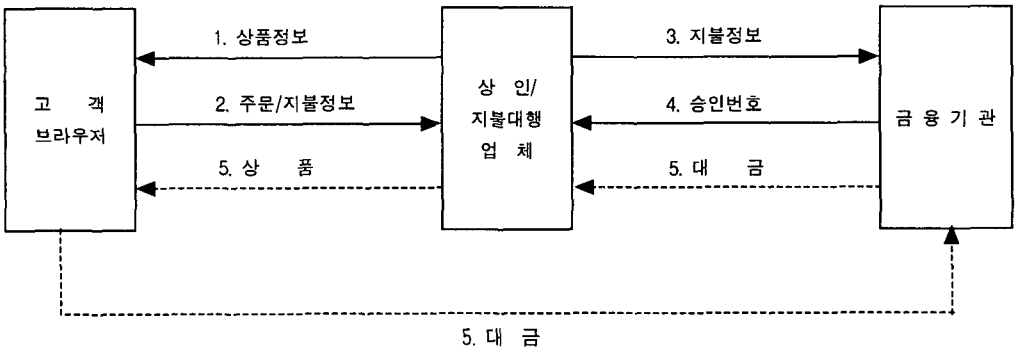
and Visa, 1997], MetaLand 결제 시스템[송용욱, 이재규, 1999], Visa Cash, Modex 등은 실제로 구현되어 사용되었거나 사용되고 있다. 그렇지만, 대부분의 경우 기술적 우월성과 상관없이 구현의 복잡성이나 사용상의 어려움 등의 이유로 시장진입에 실패하였거나 시장점유율의 확보에 어려움을 겪고 있고, 우리나라를 포함한 대부분의 나라에서는 SSL 기반의 신용카드 전자지불시스템에 의한 결제가 전자상거래 결제의 대부분을 차지하고 있다[통계청, 2003].

지금까지 살펴본 바와 같이 기존의 전자지불시스템 관련 연구들은 전자지불시스템 분류나 비교 연구 등 현황 및 성공 요인에 대한 것들이 대부분이며, 또한 전자지불시스템 프로토콜과 모형들도 기술적 우월성에만 초점을 맞춘 나머지 일반화에 성공한 사례가 없으며, 전자상거래 초기부터 도입된 SSL 기반 신용카드 전자지불시스템이 그 장단점에 대한 뚜렷한 분석도 없이 현재까지도 일반적으로 사용되고 있다. 따라서, 본 연구에서는 SSL 기반 신용카드 전자지불시스템의 장단점을 암호학의 이론적인 측면과 함께, 실제 범죄사례들을 바탕으로 하여 실제적 측면에서도 살펴본 후, 그 문제점을 해결할 수 있는 전자지불시스템 구조를 제시하고자 한다. 이를 위하여 다음 절에서는 SSL 기반 신용카드 전자지불시스템에 대하여 살펴보도록 하겠다.

2.2 신용카드 전자지불시스템

현재 우리나라 대부분의 신용카드 지불시스템이 채택하고 있는 구조는 (그림 1)과 같다. 이런 구조의 지불시스템을 보통 "SSL 기반 시스템"이라고 부르고 있는데, 그 이유는 (그림 1)의 2번 메시지(주문/지불정보)가 웹 브라우저에 내장된 SSL 보안 기능에 의하여 암호화되어 전달되기 때문이다. (그림 1)의 SSL 기반 시스템에서 2번 메시지의 내용중 지불정보로 보통 사용되는 것이 신용카드번호와 카드유효 기간이다. 초기 신용카드 지불시스템 시절부터 흔히 문제시 되었던 것이 2번 메시지의 내용이 인터넷 상에서 제 3자에게 도청되어 노출되는 것, 즉 기밀성(Confidentiality)의 문제였다. 이 때문에 Netscape사가 SSL을 웹상에 구현하여 제공하기 시작하면서 신용카드 전자지불시스템에 SSL을 즉시 활용하였고, 또한 SSL에서 사용하는 암호화 키 크기가 40bit로 너무 작은 점이 문제가 되어 그 동안 그것을 128bit로 증가시키는 것이 현안이 되어왔다.

그렇지만, SSL은 기본적으로 웹 서버와 웹 브라우저 간의 기밀성, 인증(Authentication) 및 무결성(Integrity)을 위한 보안 프로토콜로서[Freier et. al., 1996] 전자지불시스템을 염두에 두고 만들어진 것이 아니다. (그림 1)을 보면 2번 메시



(그림 1) SSL 기반 신용카드 지불시스템의 구조

지를 받은 상인 또는 지불대행업체[1]는 지불정보를 다시 3번 메시지를 통하여 금융기관에 전달하고 있는데, SSL이 고객의 웹 브라우저와 상인(또는 지불대행업체)의 웹 서버 간에만 기밀성을 보장하므로 상인(또는 지불대행업체)은 지불 정보의 전달과정에서 고객의 지불 정보를 볼 수 있으며, 또한 웹 브라우저에 대한 인증이 고객에 대한 인증을 의미하는 것이 아니므로 신용카드 번호, 유효기간 등 고객이 웹 브라우저에 입력한 정보 외에는 고객을 인증하는 별도의 방법이 없다. 이론적으로 볼 때, SSL 기반 신용카드 전자지불시스템의 가장 큰 문제점으로 지적되는 것이 상인(또는 지불대행업체)에 대한 고객 지불정보의 노출과 인증 메커니즘의 부재이다. 이 부분을 해결하기 위하여 SET(Secure Electronic Transaction)에서는 지불정보를 금융기관의 공개키로 암호화함으로써 상인이 지불정보에 접근하지 못하게 하고, 대신에 고객과 상인 간의 결제 합의를 증빙하기 위하여 이중서명(Dual Signature)를 사용하였다[Master Card and Visa, 1997 ; 송용욱, 1997 ; 송용욱, 이재규, 1999]. 그러나, 이러한 기술적 우월성에도 불구하고 고객이 웹 브라우저 외의 별도 시스템을 설치하여 사용하여야 하는 사용상의 불편, 구현의 복잡성, 서버에 대한 과중한 부하 등의 이유로 상업화에는 실패한 바 있다.

전술한 이론적 한계에도 불구하고, SSL 기반 신용카드 전자지불시스템이 현재 가장 많이 쓰이고 있는 이유는 구현상의 단순성 때문인 것으로 보여진다. SSL에 의한 보안은 웹 브라우저와 웹 서버 간에 자동적으로 이루어지기 때문에 지불시스템 개발자가 별도로 구현해야 할 것이 없다. 또한, 웹 브라우저만을 이용하므로 고객에 대한 특별한 사용법 교육이 필요 없고, 전자상거래 초기부터 사용되어 왔기 때문에 고객들에게 친숙하다는 것도 그 이유로 꼽을 수 있을 것이다.

그렇지만, 전술한 이론적 한계를 무시한 채 SSL 기반 신용카드 전자지불시스템을 계속 사용해야 하는 것인지는 다시 생각해 보아야 할 문제이며, 또한 실제적 사용에는 문제가 없었는지를 살펴보고 그에 대한 대책을 세울 필요가 있는 것으로 생각된다. 따라서, 다음 절부터는 지금까지 이야기한 SSL 기반 신용카드 전자지불시스템의 이론적 한계 외에 실제적 측면에서의 문제점을 기존의 사건, 사고를 바탕으로 살펴보고자 한다.

3. 우리나라 전자지불시스템 현황

실제적 측면에서 SSL 기반 신용카드 전자지불시스템의 문제점을 알아보기 위하여 본 연구에서는 사건 및 사고 뉴스 조사, 인터넷 쇼핑몰 방문 인터뷰 등을 시행하였다. 먼저 전자쇼핑몰 및 지불대행업체의 결제 또는 보안 담당자와 인터뷰를 실시한 결과를 살펴보도록 하겠다. 2001년 3월부터 5월에 걸쳐 4개의 종합쇼핑몰, 3개의 전문몰 그리고 3개의 지불대행업체를 대상으로 인터뷰를 실시한 결과 조사된 기관별 사고 상황이 <표 1>에 정리되어 있다.

인터뷰 결과만을 보면 신용카드에 의한 사고가 전자지불시스템 사고의 전부를 차지한다. 종합쇼핑몰 B, C, D의 경우 2000년 10월 또는 12월 이후에 한 건의 사고도 없는 것으로 보고되는 것은 그때를 기준으로 신용카드 전자지불시스템의 입력 내용을 바꾸었기 때문인 것으로 파악된다. 이때를 기준으로 신용카드 전자지불시스템들은 기존에 신용카드번호와 유효기간 만을 입력 받던 것에 추가하여 카드소지자의 주민

1) 우리나라 여신전문금융업법 제 2조에서는 결제대행업체(PG, Payment Gateway)에게 상인과 마찬가지로 가맹점의 지위를 부여하고 있다[재정경제원, 2002].

〈표 1〉 인터뷰 기관별 사고 상황

분 야	기 관	사 고 상 황	사고 지불수단	비 고
종합쇼핑몰	A	0 건		
	B	1.2건/년 (2000년 10월 까지) 0 (2000년 10월 이후)	신용카드	2000년 5월 이후 급속히 사고 증가
	C	4~6건/년 (2000년 10월 까지) 0 건 (2000년 10월 이후)	신용카드	
	D	3건 (2000년 8월~2000년 11월) 0건 (2000년 12월 이후)	신용카드	
전 문 몰	E	0건		
	F	0건		서버해킹 2건
	G	총 1건	신용카드	
지불대행업체	H	0.01~0.02 % (거래건수 대비 사고율)	신용카드	신용카드대행업체
	I	4건/년	신용카드	신용카드대행업체
	J	0건		전자현금대행업체 서버해킹 1건

등록번호 뒤 7자리 또는 카드 비밀번호 앞 2자리도 입력 받기 시작하였으며, 그와 때를 같이하여 신용카드에 의한 사고가 사라졌기 때문이다.

그러나, 위와 같은 추가 정보 입력을 요구하지 않은 전자지불시스템들은 지불 사고로부터 자유롭지 못하였다. 실제로 서울/연합뉴스 2001년 6월 30일자 기사("해킹 개인정보로 물품 구입")나 중앙일보 200년 2월 23일 기사("카드 전표 잘못 버리면 낭패") 등은 신용카드 정보를 해킹하거나 쓰레기통에 버려진 신용카드 매출 전표를 뒤져 얻은 정보를 이용하여 신용카드번호와 유효기간의 입력만을 요구하는 전자쇼핑몰에서 일으킨 지불 사고들을 기사화한 것들이다.

인터뷰 결과와 사건 기사를 바탕으로 볼 때 지금까지의 전자지불시스템 지불 사고는 인터넷을 통해 전달되는 지불정보를 도청하거나 변경하는 고도의 정보통신 기술을 사용한 것이 아니라, 해킹 또는 길거리에서 쉽게 얻을 수 있는 기본 정보(신용카드번호, 유효기간)를 이용한 것들이다. 따라서, 우리나라 전자쇼핑몰들에서 일어나는 전자지불사고들은 카드소지자 본인 확인을 위한 깊이 있는 정보를 요구하지 않고 기초적인 정보만을 입력 받아 처리한 결과이며, 이것은 현재까지의 전자지불시스템 사고의 원인이 인증(Authentication) 문제에 있음을 밝혀주는 것이다.

그런데, 주민등록번호나 신용카드 비밀번호 등 지불정보의 내용을 추가 입력하도록 함으로써 지불 사고가 사라졌으므로 전자지불시스템의 인증 문제가 완전히 해결된 것일까? 여러 가지 정황을 살펴 본다면 그렇지 않은 것을 알 수 있다. 우선 논리적으로 생각해볼 때 주민등록번호나 신용카드 비밀번호가 인증을 위한 확실한 도구가 되지 않는다는 점이다. 주민등록번호는 공공기관, 금융기관의 각종 서식이나 이력서 등에서 자주 사용되는 것이고, 주민등록증 자체도 외부에 많이 노출되는 신분증이다. 그리고, 비밀번호의 경우에는 전체 4자리 중 2자리만을 입력받으므로 가능한 키의 값이 00에서 99까지 100개에 불과하기 때문에 쉽게 노출 될 수 있다[2].

2) 비밀번호를 앞 2자리만 입력 받는 이유는 그것을 입력 받아 처리하는 상인 또는 지불대행업체가 가맹점의 위치에 있으며 신용카드사의 Trusted-third Party의 위치에 있지는 못하기 때문이다. 비밀번호 4자리가 제3자에게 노출되면 신용카드사는 현금 서비스

실제적인 측면에서는 개인의 신용카드정보 유출 사고가 적지 않게 일어난다는 점이 또한 주민등록번호나 비밀번호의 도용에 의한 지불사고의 가능성을 시사한다. 전화가입자의 개인정보 유출 사고[매일경제, 2001. 1. 13], 개인정보 해킹 사고[전자신문, 2001. 4. 13], 인터넷 기업이나 신용카드사 직원에 의한 개인정보 유출 사고[전자신문, 2001. 9. 17 ; 조선일보, 2001. 4. 12 ; 한국경제, 2001. 4. 26] 등은 해킹이나 도덕적 해이에 의한 개인 신용정보의 유출 사고들을 기사화한 것들이다. 또한, 한국정보진흥원[2003. 7] 통계 자료에 따르면 시스템 침해 사례가 2002년 10,784건에서 2003년 7월 현재 16,782건으로 증가하고 있으며, 이는 해킹에 의한 신용정보유출의 문제도 심각하게 고려할 필요를 느끼게 한다.

특히, SSL 기반 신용카드 지불시스템의 구조 측면에서 보면 신용카드정보 유출과 관련한 문제점들이 더 많이 드러난다. 2절에서 설명한 바와 같이 SSL 기반 신용카드 지불시스템에서 상인 또는 지불대행업체는 고객의 지불정보를 볼 수 있도록 되어 있다. 이것은 두 가지 측면에서 문제로 나타난다. 첫째, 대부분의 상인 또는 지불대행업체가 고객의 지불정보를 추후 정산과정에서의 고객과의 마찰에 대비하여 자신의 데이터베이스에 저장한다는 점이다. 결과적으로 고객의 개인 신용정보가 신용카드사뿐만 아니라 여러 상인 또는 지불대행업체에도 남아있게 됨으로써 정보 유출의 가능성이 커지게 된다. 둘째, 지불시스템에서 획득한 고객의 신용정보를 상인 또는 지불대행업체가 그대로 다른 쇼핑몰에서 도용할 수 있다는 점이다. PKI(공개키 기반 구조) 기반의 전자서명은 다른 사람이 그 내용을 볼 수는 있어도 도용할 수는 없다는 점과 비교하여 생각하기 바란다. 유령 인터넷 쇼핑몰에 대한 중앙일보[2000. 3. 7]의 기사는 유령 인터넷 쇼핑몰 개설자에 의한 고객 신용정보의 절취, 유출 및 도용에 대한 우려를 더욱 크게 한다.

지금까지의 논의를 바탕으로 볼 때 우리나라 전자지불시스템의 지불 사고는 인증의 부재에서 비롯된 것이며, 전자지불시스템의 인증 문제가 아직 완전히 해결된 상태도 아니다. 그렇지만, 인증 문제를 해결하기 위하여 이미 상업적으로 실패한 SET의 전철을 밟을 수도 없다. 따라서, 본 연구에서는 SET와 같은 복잡한 암호화 기법을 쓰지 않으면서도 인증의 문제를 해결할 수 있는 전자지불시스템 구조를 제안하고자 한다.

4. 인증을 보완한 전자지불시스템 구조

3절에서 소개된 사건 사례들은 전부 카드 소지자 인증의 실패에 기인한 것들이다. 이러한 인증 실패의 원인은 인증 방법으로써 신용카드 번호, 유효기간 등 일반적으로 쉽게 노출될 수 있는 정보만을 사용하였기 때문인 것으로 파악된다. 이러한 문제점의 원인으로는 두 가지 점을 생각할 수 있다. 첫째는, 상인과 신용카드사는 별개의 회사임에도 불구하고 현재의 신용카드 지불시스템의 구조상 인증 정보를 공유할 수밖에 없다는 점에 있다. 완벽한 인증을 위해서는 카드 소지자와 신용카드사 만이 아는 비밀정보를 최대한 많이 활용하여야 한다. 그렇지만, 그렇게 되면 인증 과정에서 이러한 비밀정보를 상인들도 알게 되는 것이 문제가 되며, 이것을 피하기 위해서는 다시 인증을 위한 비밀정보를 최소한으로 해야 하는 딜레마에 빠지게 된다. 인증을 위한 추가 정보로 주민등록번호와 카드 비밀번호를 입력 받는 제도를 시행하면서 카드 비밀번호 앞 2자리만을 받는 것도 이러한 딜레마를 반영한 결과이다. 그렇지만, 주민등록번호와

스 사고의 발생에 직면하게 된다.

카드 비밀번호를 입력 받는다 해도 이것이 쇼핑몰의 데이터베이스에 저장되는 한 시스템 해킹 또는 고의 유출에 의한 정보노출의 위협은 계속 남아있게 된다. 둘째 이유는 시스템의 단순화이다. PKI 기반의 전자서명과 이중서명 등을 활용하면 현재의 신용카드 지불시스템의 구조에서도 상인에게 신용카드 관련 정보를 노출하지 않고도 완전한 인증이 가능하다. 하지만, 이를 위해서 시스템은 복잡해 질 수 밖에 없게 되며, 그 대표적인 실패사례로서 SET을 들 수 있다.

인증 문제 및 SET에서와 같은 시스템 복잡성의 문제는 현재 신용카드 지불시스템의 구조에서 지불 정보가 상인(또는 지불대행업체)을 경유해 금융기관에 전달되는 정보 흐름의 구조를 변경함으로써 해결할 수 있다. 즉, 기존의 지불시스템 구조에서 보여지는 "주문정보와 지불정보의 통합" 구조에서 벗어나 "주문정보와 지불정보의 분리" 구조를 사용하는 것이다. 주문정보와 지불정보의 분리 구조란 지불정보가 주문정보와 함께 상인에게 전달된 후 지불정보가 다시 상인으로부터 금융기관으로 전달되는 기존의 구조[(그림 1) 참조]와 달리, 주문정보는 기존처럼 고객으로부터 상인에게 전달되지만 지불정보는 별도로 고객으로부터 금융기관에 직접 전달되는 구조이다. 다만, 이 경우 이렇게 분리된 지불정보와 주문정보 간의 연결성(Linkage)을 상인이(지불정보의 내용을 모른 상태에서) 확인할 수 있어야 하는 문제가 발생한다. 즉, 특정 주문에 대한 결제가 원래의 주문 금액대로, 그리고 중복됨이 없이 올바로 처리되었음을 상인이 확인할 필요가 있는 것이다. 주문정보와 지불정보를 분리하면서 상인에 의한 연결성 확인을 가능하게 하기 위하여 본 연구에서 제시하는 전자지불시스템 구조가 (그림 2)에 나타나 있다.

(그림 2)에서 각 메시지의 내용은 다음과 같다.

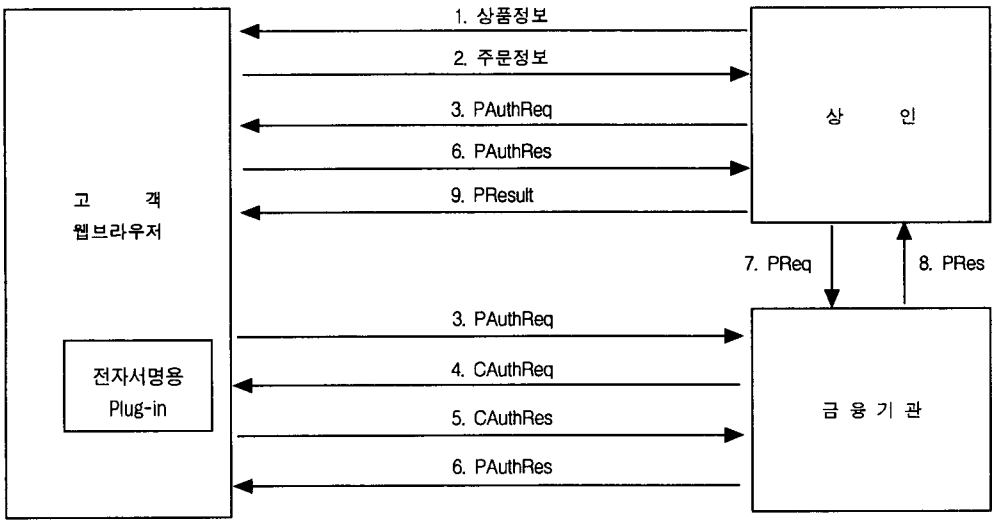
PAuthReq = {상인이름, 거래번호, 결제금액, 상인 Id, 상인 URL}

CAuthReq = {상인이름, 거래번호, 결제금액}

CAuthRes = {지불정보, {Id, Password}|{전자서명}}

PAuthRes = {결제예약번호, 거래번호}

PReq = {결제예약번호, 결제금액, 상인 Id, {Password}|{전자서명}}



(그림 2) 인증을 보완한 전자지불시스템 구조

PRes={결제처리번호, 결제금액}
PResult={처리결과, 공지사항}

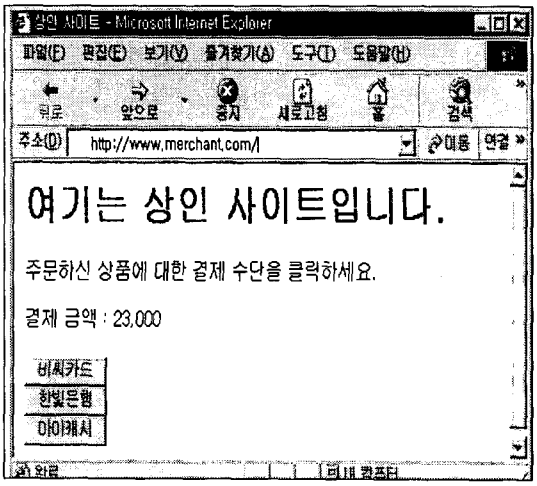
제시된 전자지불시스템의 결제 처리 절차는 다음과 같다.

(Step 1) 상품정보는 통상의 전자쇼핑몰에서처럼 상품카탈로그, 상품검색엔진 등을 이용하여 고객의 웹 브라우저를 통해 제공한다.

(Step 2) 주문정보는 통상의 전자쇼핑몰에서처럼 장바구니 등을 이용하여 고객의 웹 브라우저로부터 받는다.

(Step 3) 고객이 결제를 요구하면 상인 시스템은 그 상인 시스템에 고유한 거래번호를 생성한 후 상인이름, 결제금액, 금융기관으로부터 사전에 받아둔 상인 Id, 상인 URL 등과 함께 PAuthReq 메시지에 담아 고객의 웹 브라우저를 경유하여 금융기관 웹 서버에 전달하고, 고객의 웹 브라우저에 금융기관 웹 사이트가 나타나도록 한다.

이것은 기술적으로는 웹의 Form 태그와 JavaScript나 VBScript와 같은 클라이언트측 스크립트를 이용하여 가능하다. 예를 들어 (그림 3)과 같은 결제화면에서 거래번호, 결제금액 등이 금융기관으로 전달되면서 금융기관 웹 사이트가 고객의 웹 브라우저에 나타나게 하려면 (그림 4)와 같은 HTML 파일을 상인 시스템이 제공하면 된다.



(그림 3) 상인 시스템의 결제 화면

```
<html> <head> <title>상인 사이트</title>
<SCRIPT LANGUAGE = "JavaScript">
<!-- function Call(form, url) { form.action = url ; form.submit(); } //-->
</SCRIPT> </head> <body>
<h1> 여기는 상인 사이트입니다</h1>.
주문하신 상품에 대한 결제 수단을 클릭하세요 <br> <br>.
결제 금액 : 23,000<br>
<form name = formname method = post>
<input type = hidden name = TransactionId value = M200202010011>
<input type = hidden name = Amount value = 23000>
<input type = hidden name = MerchantURL value = "http://www.merchant.com/SXT">
<input type = button value = "비씨카드" OnClick = 'Call(this.form, "http://www.bccard.co.kr/SCT")'>
<br>
<input type = button value = "한빛은행" OnClick = 'Call(this.form, "http://www.ehanvit.co.kr/SDT")'>
<br>
<input type = button value = "아이캐시" OnClick = 'Call(this.form, "http://www.icash.co.kr/SMT")'>
<br>
</form> </body> </html>
```

(그림 4) 상인 결제 화면의 소스 코드

(그림 4)에서 비씨카드, 한빛은행, 아이캐시 중 원하는 지불수단을 고객이 클릭하면 JavaScript의 Call 함수가 해당 금융기관 사이트를 부르면서 Hidden 필드의 거래번호(TransactionID, M200202010011)와 결제금액(Amount, 23000) 및 상인의 URL(MerchantURL, http://www.merchant.com/SXT) 등 PAuthReq 메시지를 POST 메소드로 넘기고 있는 것을 볼 수 있다.

(Step 4) 금융기관 사이트에서 고객은 금융기관과 직접 인증정보를 교환(CAuthReq, CAuthRes)하면서 올바른 금융 고객인지를 인증하게 된다.

이 과정에서 금융기관의 웹 페이지는 자신이 금융기관의 웹 페이지임을 확실하게 보여 줌으로써 고객의 신뢰를 확보하고 Man-in-the-middle 공격[Schneier, 1996]과 같은 정보 도청 시도에 대비해야 한다. 그 방안으로는 고객 웹 브라우저의 주소 입력 부분에 금융기관의 URL이 나타나게 하거나, 인증정보 입력 화면에 그 금융기관의 로고 등을 보여주는 것들이 있다. 또, PAuthReq 메시지로 넘어온 상인이름과 결제금액을 고객의 웹 브라우저에 디스플레이 하여 고객이 자신의 주문내용을 재확인할 수도 있다. 또한, 인증용 정보로는 신용카드번호나 유효기간, 계좌번호 같은 상대적으로 노출 가능성이 높은 지불정보 외에도 고객이 금융기관에 사전에 등록한 Id, Password 또는 PKI 기반의 전자서명을 이용하여 인증을 수행한다. 또한, 이 과정에서 상인 시스템은 완전히 배제되기 때문에 상인은 지불정보로부터 자유로워질 수 있다.

(Step 5) 고객의 인증이 끝나면 금융기관 시스템은 그 금융기관 시스템에 고유한 결제예약번호를 생성한 후 상인 시스템이 보냈던 거래번호와 함께 PAuthRes 메시지에 담아 고객의 웹 브라우저를 경유하여 상인의 웹 서버에 전달하고, 고객의 웹 브라우저에는 상인의 웹 사이트가 나타나도록 한다.

이 과정은 (Step 3)과 유사한 Redirection 방법을 사용하면 된다. 단, (Step 3)의 방법을 사용할 경우 고객이 불필요하게 버튼을 한번 더 클릭을 하여야 하므로, 다음과 같이 HTTP 응답 메시지의 Location 헤더[3]를 사용하는 방법을 생각해볼 수도 있다.

HTTP/1.0 200 OK
Location : http://www.merchant.com/SXT?ReservationNo=B200202010003&TransactionId=M200202010011

금융기관 시스템이 (Step 4)의 인증과정 중 CAuthRes 메시지에 대하여 결제예약번호 생성 후 그 응답 메시지로서 위와 같은 메시지를 보내면 고객의 웹 브라우저는 바로 상인의 웹 사이트(http://www.merchant.com/SXT)를 연결하면서 GET 메소드를 통하여 결제예약번호(ReservationNo, B200202010003)와 거래번호(TransactionId, M200202010011)를 전달한다.

(Step 6) (Step 5)를 통해 결제예약번호와 거래번호를 받은 상인의 웹 서버는 거래번호를 이용하여 그 결제금액을 데이터베이스로부터 얻어낸 후 결제금액, 결제예약번호 및 상인 Id, Password 또는

3) Location 헤더가 포함된 HTTP 응답 메시지를 받은 웹 브라우저는 응답 메시지의 내용을 윈도우에 디스플레이하는 것이 아니라, Location 헤더에 나타난 주소(URL)의 웹 페이지를 다시 요구하여 그 응답 메시지의 내용을 윈도우에 디스플레이 하도록 되어 있다. 따라서, 위 예제에서처럼 금융기관 웹 서버의 응답내용을 디스플레이하는 것이 아니라 Location 헤더에 표시된 "http://www.merchant.com/SXT…" 페이지의 내용을 디스플레이하게 된다.

전자서명과 함께 PReq 메시지에 담아 금융기관 시스템에 보내어 결과를 문의한다.

(Step 7) PReq 메시지를 받은 금융기관 시스템은 먼저 상인 Id, Password 또는 전자서명을 이용하여 인증 절차를 마친 후 결제예약번호를 이용하여 데이터베이스로부터 결제금액과 관련 지불정보를 얻어내어 두 결제금액이 일치하는지를 확인한 후 지불정보와 상인 Id로부터 얻어진 상인의 결제정보를 이용하여 결제처리를 완료한다. 여기서 결제예약번호가 연결성을 확보하는 수단이 된다. 그리고, 그 결제처리번호를 생성하여 결제금액과 함께 PRes 메시지에 담아 상인 시스템에 돌려준다.

(Step 8) 상인 시스템은 결제처리번호를 확인하여 결제처리가 완료되었는지를 확인하고, 결제금액의 일치여부를 다시 확인한 후 고객의 웹 브라우저에 처리결과 및 앞으로의 배송 일정정보 등 공지사항 등을 포함한 PResult 메시지를 보내어 디스플레이 하도록 한다.

5. 토 의

위 지불시스템 구조에서 1번, 2번, 9번 메시지는 단순 정보에 불과하므로 기밀성, 인증, 무결성 등 보안이 필요 없다. 3번 메시지는 무결성이 필요하다. PAuthReq의 내용 중 상인이름은 4번 과정에서 디스플레이를 위한 용도이므로 민감한 정보가 아니다. 거래번호와 결제금액은 3번에서 외부에 노출되어도 아무런 문제가 없고, 만약 변경이 된다면 7번, 8번 과정에서 중복검사가 이루어지므로, 최악의 경우 지불이 이루어지지 않을 수는 있어도, 지불이 이루어지고도 상인이 그 사실을 몰라서 상품을 배송하지 않는 경우는 발생하지 않는다. 다만, 상인 Id와 상인 URL이 변경이 된다면 구매대금이 다른 상인에게 지불되는 것이 가능하다. 그러나, 이것은 고객이 그렇게 할 이유는 없고 제 3자가 하는 경우이므로, SSL을 사용하면 쉽게 해결된다.

4번 및 5번 메시지는 기밀성, 인증, 무결성 등이 요구된다. 기밀성과 무결성의 경우는 웹에 내장된 SSL만으로도 충분히 이루어질 수 있다. 인증의 경우에는 신용카드번호, 유효기간 외에 주민등록번호나 카드비밀번호 만으로도 어느 정도 확보되고 좀 더 확실한 방법으로는 Id/Password 또는 전자서명을 사용할 수도 있다.

6번 메시지도 기밀성, 인증, 무결성 등 보안이 필요 없다. 결제예약번호가 변경되더라도 7번, 8번 과정에서 중복 검사가 이루어지므로 지불이 완료되지 않을 수는 있어도, 잘못 지불되지는 않는다. 결제예약번호가 노출되어 다른 사람이 다른 상인 Id를 이용하여 7번, 8번 과정을 수행함으로써 대신 지불 받으려고 시도하더라도 상인 Id에 대한 중복검사가 이루어지므로 역시 지불이 완료되지는 않는다.

7번 및 8번 메시지는 기밀성, 인증, 무결성 등이 요구된다. 이를 위하여 4번, 5번 메시지에서처럼 SSL과 상인 Id에 대한 Password를 사용하는 방식을 사용할 수도 있고, 아니면 PKI 기반의 전자서명을 도입할 수도 있다. 결제 예약번호의 기밀성은 문제가 되지 않는다. 7번 메시지에 의하여 결제예약번호가 노출된 상태에서 네트워크나 서버의 문제에 의하여 8번 메시지까지 처리가 완료되지 못하여 상인 시스템이 7번 메시지를 재시도하는 사이에 제 3자가 먼저 7번 및 8번 과정을 마칠 수도 있다. 그러나, 이것은 앞 절에서 설명하였듯이 상인 Id에 대한 중복 검사를 통하여 방지할 수 있으므로 문제가 되지 않는다.

6번 과정에서 아주 짧은 메시지인 결제 예약 번호와 거래번호만이 전달되는 것은 이 전자지불시스템 구조를 모바일 인터넷에서도 사용가능 하게 한다. 모바일 인터넷은 아직 전자서명과 같은 긴 메시지를 처리할 수 없으나, 전자서명 대신 Id/Password를 사용할 경우 이 전자지불시스템은 고객과 상인 및 금융기관 시스템 간에 짧은 메시지만을 전달하도록 되어있으므로, 이 전자지불시스템 구조를 변경 없이 그대로 사용 가능하다.

본 연구에서 제시한 전자지불시스템 구조의 장점은 그 단순성에 있다. 전자서명과 같은 복잡한 과정은 최소화되었으며, 기존의 SSL 기반 위에 Id, Password 만을 이용하여도 소기의 보안효과를 얻을 수 있다. 또한, 이 구조는 신용카드, 전자자금이체, 서버형 전자현금, 가상계좌 시스템, 모바일 인터넷 등에서 변경 없이 그대로 사용할 수 있다. 신용카드의 경우에는 금융기관 위치에 신용카드사 또는 그 TTP(Trusted Third

Party)가 위치하면서 결제처리번호로 카드승인번호를 보내주면 되고 전표 매입(Capture) 처리는 기존의 방법과 마찬가지로 사후에 일괄 처리하면 된다. 전자자금이체의 경우에는 금융기관 위치에 은행 또는 그 TTP가 위치하면서 결제처리시 계좌이체를 수행하면 되고 그 계좌이체 거래에 대한 고유번호를 결제처리번호로 보내주면 된다. 서버형 전자현금의 경우에는 금융기관 위치에 전자현금 서비스업체가, 가상계좌 시스템의 경우에는 가상계좌 서비스업체가, 모바일 인터넷의 경우에는 그 결제의 성격에 따라 핸드폰 결제이면 이동통신업체가, 계좌이체이면 은행이 위치하면 된다.

지금까지의 논의를 바탕으로 본 연구에서 제시한 전자지불시스템 구조를 SSL 기반 신용카드 지불시스템 및 SET와 비교하면 <표 2>와 같다.

6. 결 론

현재 우리나라 전자쇼핑몰 또는 지불대행업체들이 전자지불시스템 보안과 관련하여 강조하는 것은 지불 정보의 네트워크 보안 및 그 암호화 키의 크기이다. 네트워크 보안을 위하여 대부분의 전자지불시스템들은 키 크기 128Bit의 SSL 보안 기법을 사용하며, 그 점을 마케팅 측면에서도 강조하고 있다. 그렇지만, 실제로 일어나고 있는 전자쇼핑몰의 지불사고는 "부당 대금 청구", 즉, "신용카드 도용에 의한 예상치 않은 대금 청구"의 형태이며, 그러한 사고들의 경위를 살펴보면 고객의 카드정보 및 유효기간 등의 민감한 정보가 지불정보시스템의 암호화 보

〈표 2〉 지불시스템별 장·단점 비교

지불시스템 / 비교 기준	SSL 기반시스템	SET	제안 지불시스템
보 안	상인에 정보 노출 인증에 한계	기밀성, 인증, 무결성, 연결성 보장	기밀성, 인증, 무결성, 연결성 보장
개발 용이성	용 이	어려움	용 이
시스템 부하	적 음	많 음	적 음
사용 용이성	용 이	어려움	용 이
적 용 지 불 수 단	신용카드	신용카드(다른 지불수단에 확장가능)	신용카드, 전자자금이체, 서버형 전자현금, 가상계좌시스템, 모바일 인터넷 등

안 허점을 통하여 유출되기 보다는 고객의 부주의나 쇼핑몰, 지불대행업체 또는 금융기관의 시스템 보안 허점을 통하여 유출된 사례들이 전부를 차지하고 있다. 따라서, 본 연구에서는 현재의 우리나라 전자지불시스템의 구조 분석을 통하여 민감한 지불 정보의 유출 가능 통로를 파악하고, 현재까지의 전자지불시스템들의 사고 사례를 조사하여 실제로 사고가 빈발하고 있는 지불 정보 유출 통로를 찾아냄으로써 그 문제점을 파악하고, 나아가 이러한 문제점을 해결할 수 있는 전자지불시스템 보안 구조를 제시하였다.

먼저, 본 연구에서는 우리나라 전자상거래 결제에서 가장 많이 쓰이고 있는 SSL 기반 신용카드지불시스템을 이론적으로 분석하고, 실제적 측면에서의 문제점을 알아보기 위하여 사건 및 사고 뉴스 조사, 인터넷 쇼핑몰 방문 인터뷰 등을 시행하였다. 그 결과로써 인증의 문제가 현 전자지불시스템에서 가장 큰 문제임을 도출하고, 인증 문제를 해결하면서 SET에서와 같은 시스템 복잡성 및 사용상의 어려움도 극복하기 위하여 "주문정보와 지불정보의 분리"가 필요함을 인식하고 고객과 금융기관 간에 직접 지불정보를 주고받도록 하는 전자지불시스템 구조를 제시하였다. 이 전자지불시스템 구조에서 각 메시지는 기밀성, 인증, 무결성 등 파악된 필요 요건에 맞추어 암호화 처리되고, 고객 시스템이 웹 브라우저 내에 구현 될 수 있도록 되어 있으며, 상인을 지불정보로부터 자유롭게 하고, 상인 시스템의 구조를 단순화함과 동시에 그 부하를 절감할 수 있도록 하였다. 이 전자지불시스템 구조는 신용카드, 전자자금이체, 서버형 전자현금, 가상계좌 시스템, 모바일 인터넷 등 다양한 전자지불시스템에서 변경 없이 그대로 사용할 수 있다.

참 고 문 헌

[1] 김은영, 조동섭, "쇼핑몰을 위한 혼합형 전자지불시스템", *2000년도 한국정보과학회 가을 학술발표논문집*, 제27권 2호, 2000년, pp. 245-247.

[2] 김종률, "전자상거래에서 IC 카드 소프트웨어 및 활용방안 연구", *정보화 저널*, 제3권 4호, 1996년 12월, pp. 55-65.

[3] 김종우, 송주석, "전자 지불 프로토콜 표준화 동향", *통신정보보호학회지*, 제10권 2호, 2000년 6월, pp. 33-42.

[4] 김창수, 홍일유, "전자지불시스템의 비교분석을 위한 프레임웍", *경영정보학연구*, 제8권 3호, 1998년 12월, pp. 147-163.

[5] 문종진, "전자화폐시대의 도래에 따른 영향과 대응", *전자화폐 세미나 발표자료*, 한국경제신문사, 1996. 7.

[6] 송용욱, "전자상거래와 SET 프로토콜", *컴퓨터월드*, 1997년 11월, pp. 248-252.

[7] 송용욱, 이재규, "메타-몰 구조를 갖는 전자쇼핑몰에서의 안전한 지불체계에 대한 연구", *Information Systems Review*, 제1권 2호, 1999년 12월, pp. 41-54.

[8] 오형근, 이임영, "전자화폐 시스템 개발 동향", *통신정보보호학회지*, 제9권 1호, 1999년 3월, pp. 13-31.

[9] 이재규, "전자상거래의 전망과 연구 주제", *'97 한국경영정보학회 춘계학술대회 논문집*, 1997. 6.

[10] 이재규, 권순범, 김우주, 김민용, 송용욱, 최형림 편저, *전자상거래원론*, 제3판, 법영사, 2002. 9.

[11] 임신영, 조현규, 함호상, 김태윤, "전자상거

래의 전자지불 기술", *정보과학회지*, 제18권 7호, 2000년 7월, pp. 28-35.

[12] 재정경제원, 여신전문금융업법, 법률 제6705호, 개정 2002. 8. 26.

[13] 제일금융연구원, *새로운 돈의 혁명 전자화폐*, 한국경제신문사, 1997. 4.

[14] 주재훈, "한국의 전자상거래 환경을 고려한 전자지불 시스템 성공요인 분석", *경영정보학연구*, 제9권 1호, 1999년 3월, pp. 77-98.

[15] 통계청, *2003년 6월 및 2/4분기 사이버쇼핑몰통계조사 결과*, 2003. 8. 5.

[16] 통계청, *전자상거래통계조사 결과(2001년 12월 및 연간 사이버쇼핑몰조사)*, 2002. 2.

[17] 한국소비자보호원 전자상거래 지원센터, *인터넷 쇼핑몰업과 소비자 보호*, 2002. 8.

[18] 한국소비자보호원, *2000년 전자상거래 소비자 상담, 피해 분석*, 2001. 2. 19.

[19] 한국정보보진흥원, *2003년 7월 해킹바이러스 통계 및 분석 월보*, 2003. 7.

[20] 홍일유, 김창수, 편완주, "전자지불시스템의 유형별 특성 분석 및 선정모형 개발", *'97 International Conference on SI Technology and Applications*, 한국경영정보학회, 1997, pp. 894-910.

[21] Abad-Peiro, J.L., N. Asokan, M. Steiner, and M. Waidner, "Designing a Generic Payment Service", *Research Report of IBM Research Division*, 1996.

[22] Asokan, N., P. Janson, M. Steiner, and M. Waidner, "Electronic Payment Systems", *Research Report of IBM Research Division*, 1996.

[23] Bellare, M., J.A. Garay, et. al., "iKP Family of Secure Electronic Payment Protocol", 1995, http://www.zurich.ibm.com/technology/security/extern/ecommerce/.

[24] Bohle, K., "The Potential of Server-based Internet Payment Systems-An Attempt to Assess the Future of Internet Payments", *Background Paper No. 3, Electronic Payment Systems Observatory (ePSO)*, Institute for Prospective Technological Studies, July 2001.

[25] Brahm, J. and E. Turban, "Electronic Card Payment Systems in Electronic Commerce", *Proceedings of International Conference on Electronic Commerce '98*, ICEC, 1998, pp. 216-223.

[26] Brands, S., "Electronic Cash on the Internet", *Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security*, Feb. 1995.

[27] Camp, L.J., M. Sirbu, and J.D. Tygar, "Token and Notational Money in Electronic Commerce", 1996, http://www.cs.cmu.edu/afs/cs.cmu.edu/user/jeanc/www/usenix.html.

[28] Chung, E. and D. Dardailler, "White Paper : Joint Electronic Payment Initiative (JEPI)", 1997, W3C, http://www.w3.org/ECommerce/white-paper.html.

[29] Clifford, B. and T. Ts'o, "Kerberos : An Authentication Service for Computer Networks", *IEEE Communications*, Vol. 32, No. 9, 1994, pp. 33-38.

[30] Cousins, S., S. Ketchpal, Paepcke, A. et. al., "InterPay : Managing Multiple Pay-

ment Mechanisms in Digital Libraries", A Project in the Stanford Digital Library, 1995, http://robotics.stanford.edu/~ketchpel/diglib/interpay.html.

[31] Crede, Andreas, "Electronic Commerce and the Banking Industry : The Requirement and Opportunities for New Payment Systems", *Journal of Computer-Mediated Communication*, 1996.

[32] Cross-Industry Working Team, "Electronic Cash, Tokens and Payments in the National Information Infrastructure", 1996, http://WWW.CNRI.Reston.VA.US : 3000/XIWT/documents/dig_cash_doc/ElecCashToC.html.

[33] CyberCash, *CyberCash White Papers*, 1996, http://www.cybercash.com/cybercash/

[34] DigiCash, An Introduction to ecash, 1996, http://www.digicash.com/publish.ecash_intro/ecash_intro.html.

[35] Elgamal, T., "Commerce on the Internet : Credit Card Payment Applications over the Internet", 1995, http://home.netscape.com/newref/std/credit.html.

[36] Freier, Alan O., Philip Karlton, Paul C. Kocher, *The SSL Protocol, Version 3.0*, Internet Draft, 1996.

[37] GPayments, *Visa 3-D Secure vs. MasterCard SPA : A comparison of online authentication standards*, 2002.

[38] Hitachi Research Institute, *Electronic Money*, Hitachi America, Ltd., 1997.

[39] Kalakota, Ravi and Andrew B. Whinston. *Frontiers of Electronic Commerce*, Addison Wesley, 1996.

[40] Kienzle, J. and A. Perrig, "Digital Money : A Divine Gift or Satan's Malicious Tool?", 1996, http://didecs1.epfl.ch/~aperrig/memoirel/meroirel.html.

[41] Master Card and Visa, *Secure Electronic Transaction Specification Version 1.0*, May 1997.

[42] Medvinskey, G., and B. Clifford Neuman, "NetCash : A Design for Practical Electronic Currency on the Internet", *Proceedings of the First ACM Conference on Computer and Communications Society*, November 1993.

[43] Pays, P. and F. Comarmond, "An Intermediation and Payment System Technology", *Fifth International World Wide Web Conference*, May 6-10, 1996, Paris, http://www5conf.inria.fr/fich_html/papers/P27/Overview.html.

[44] Schneier , Bruce, *Applied Cryptography, 2nd Edition*, John Wiley & Sons Inc., 1996.

[45] Stadler, F., "Electronic Money : Preparing the Satge", Working Paper of University of Toronoto, 1997, http://www.fis.utoronto.ca/~stadler/html/e-cash.html.

[46] Visa, *3-D Secure : Protocol Specification-Core Functions v1.0.1*, 2001.

[47] 매일경제, "전화가입자 정보 MPC 유출", 2001. 1. 13.

[48] 서울/연합뉴스, "해킹 개인정보로 물품 구입", 2001. 6. 30.

[49] 세계일보, "개인정보 침해 사고 급증", 2001. 8. 12.
[50] 전자신문, "780만명 개인정보 빼낸 10대 해커 구속", 2001. 4. 13.
[51] 전자신문, "개인정보유출 27개 인터넷 기업 적발", 2001. 9. 17.
[52] 조선일보, "신용정보 9개월 간 1500만명 유출 적발", 2001. 4. 12.
[53] 중앙일보, "인터넷 쇼핑 유령회사 많다", 2000. 3. 7.
[54] 중앙일보, "카드전표 잘못 버리면 낭패", 2000. 2. 23.
[55] 한국경제, "돈 받고 개인정보 판매 카드회사 등 본격 수사", 2001. 4. 26.

저자소개

송 용 욱

한국과학기술원에서 1990년도와 1995년도에 각각 석사 및 박사학위를 취득하였으며, 현재 연세대학교 원주캠퍼스 경영·정보학부 교수로 재직하고 있다. 연구분야는 전자상거래, 전자결제 및 보안, 경영분야 문제에의 지능정보시스템 응용, 지능정보시스템과 전자상거래의 통합 등이다. 연구 논문들은 Management Science, Annals of Operations Research 등에 게재되었다.

이 재 규

서울대학교 산업공학과 학사, 한국과학기술원 산업공학과 석사, University of Pennsylvania의 The Wharton School 박사를 취득하였다. 현재 한국과학기술원 테크노경영대학원 교수 및 (사)국제전자상거래 연구센터 소장으로 재직 중이며, Journal Electronic Commerce Research and Applications의 편집장, Decision Support Systems, Expert Systems with Applications, International Journal of Electronic Commerce 등의 국제학술지에서 편집위원으로 활동하고 있다. 한편, 한국지능정보시스템학회 학회장을 역임하였고, The 3rd World Congress on Expert Systems(1996)와 International Conference on Electronic Commerce(1998, 2001)에서 학술대회장을 역임하였다. 주요 연구분야는 전자상거래와 지능정보시스템 등이다.

황 재 훈

현재 연세대학교 원주캠퍼스 경영정보학과 부교수로 재직중이다. 연세대학교 경영학과를 졸업하고, 미국 University of Nebraska-Lincoln에서 경영학박사(MIS 전공)학위를 취득하였다. 삼성 SDS에서 삼성전자의 BPR /ISP 및 ERP 구축을 수행하였다. 주요 관심분야는 ERP 및 e-비즈니스 확장 솔루션, 경영전략과 IT 전략 연계 등이다.

◈ 이 논문은 2003년 7월 1일 접수하여 1차 수정을 거쳐 2003년 8월 24일 게재확정되었습니다.