情 報 保 護 學 會 誌
第 15 卷 第 4 號, 2005. 8

SET와 그 변형기법들에 관한 연구

장 우 석*, 이 광 우*, 최 동 현*, 정 학*, 이 병 희*, 최 윤 성*, 김 승 주**, 원 동 호***

요 약

SET는 인터넷과 같은 개방형 통신망에서 안전하고 효율적인 신용카드 기반의 전자결제를 수행하기 위해 개발된 전자지불 프로토콜이다. 하지만 SET를 이용한 신용카드 기반 전자지불시스템은 사용상의 불편함과 구현의 복잡성, 서버에 대한 과중한 부하 등의 이유로 상업화에는 실패하여 SSL/TLS 프로토콜 방식이 주로 사용되고 있다. 최근에는 SSL/TLS와 SET의 장점을 모두 만족시키는 새로운 모델인 3D SET와 3-D Secure가 제시되었다. 본 고에서는 전반적인 SET 프로토콜의 개요와 SET에 사용된 보안 기술에 대해서 살펴보고, SSL/TLS 프로토콜과의 장·단점을 비교/분석한다. 그리고, SET 이후에 등장한 3D SET와 3-D Secure에 대한 동향을 분석하고, 모바일 전자상거래를 위한 Wireless SET에 대해 살펴보기로 한다.

Ⅰ. 서 론

인터넷 사용자가 폭발적으로 증가함에 따라 전자상거래는 고도의 성장기를 지나 이제 안정화 단계에 들어서 점차 우리 생활의 일부가 되어가고 있다. 특히 인터넷상에서 전자쇼핑몰, 사이버 쇼핑몰 등의 서비스가 가장 각광받는 분야로 성장하고 있다. 이와 같은 서비스를 안전하게 제공하기 위해서는 안전한 전자지불시스템의 구축이 필요한데, 전자지불시스템은 결제 방식에 따라 크게 전자화폐(Electronic Money), 신용카드(Credit Card), 전자수표(Electronic Check)로 구분할 수 있다.

전자지불의 초기 단계에서는 웹 홈페이지에서 이용자가 직접 신용카드 번호를 입력하는 방법과 전자 우편을 통해 신용카드 번호를 전송하는 방식 등을 이용하였다. 그러나, 이 방식은 신용카드 번호가 암호화되지 않은 채 네트워크상에 그대로 전송되므로 악의적인 해커에 의해 도용될 위험이 높아 그다지 많이 쓰이지 않았다. 따라서, 전송되는 지불정보가 해커로부터 도용당하는 것을 방지하기 위해 전송되는 데이터를 암호화하는 SSL[1], SHTTP[2] 등과 같은 보안 프로토콜이 제시되었다. 보안 프로토콜로 보호되는 홈페이지에서 입력된 신용카드 번호와 같은 지불정보는 암호화되어 안전하게 상인에게 전송된다. 이 방식은 사용되는 암호화키의 크기에 따라 그 안전성이 결정되는 방식으로 큰 비트의 암호화 알고리즘을 사용할 경우 높은 안전성이 유지되어 현존하는 많은 상거래 서버시스템이 이 방법을 사용하게 되었다. 특히 SSL은 Netscape사가 개발하여 자사의 Commerce Server에 적용하였으며, 그 외 OpenMarket, IBM, Microsoft 등의 상거래 서버에도 채택되었다. 그러나, 이 방법은 쇼핑몰을 운영하는 상인에게 고객의 신용카드번호가 공개되므로 나쁜 의도를 지닌 상인에 의해 고객의 지불정보가 노출되고 웹 브라우저에 대한 인증이 고객에 대한 인증을 의미하는 것이 아니므로 신용카드 번호, 유효기간 등 고객이 웹 브라우저에 입력한 정보 외에는 고객을 인증하는 별도의 방법이 없으므로 안전하고 믿을만한 전자지불의 해결책이 되지 못하였다. 이 부분을 해결하기 위해서 SET에서는 공개키로 신용카드 번호, 유효기간 등의 정보를 암호화함으로써 상인이 지불정보에 접근하지 못하게 하고, 대신에 고객과 상인 간의 결제 합의를 증빙하기 위하여 이중서명(Dual

* 성균관대학교 정보통신공학부 정보보호및암호학연구실/정보통신보호연구실({wschang, kwlee, dhchoi, hchong, bhlee, yschoi}@dosan.skku.ac.kr)
** 성균관대학교 정보통신공학부 조교수(skim@ece.skku.ac.kr)
*** 성균관대학교 정보통신공학부 정교수(dhwon@ece.skku.ac.kr)

Signature)을 사용하였다. 따라서, SET를 이용한 신용카드 기반의 전자지불시스템은 SSL을 이용했을 때보다 훨씬 더 높은 수준의 보안성을 제공하므로 SET가 인터넷상에서 카드로 지불하는데 있어서 지배적인 방법이 될 수 있을 것이라 생각하였다. 그러나, SET를 제대로 구현하는데 있어서의 기술, 시간, 비용 등의 제반적 측면과 사용자 편의성 측면, 그리고 처리 속도가 느리다는 단점 때문에 현재 인터넷상의 상거래에서 SET를 사용하는 건수는 작은 실정이다.

본 고에서는 신용카드 기반 전자지불시스템에 사용되는 SET에 관해 전반적으로 살펴보고, 전자상거래 초창기부터 현재까지 사용되고 있는 SSL/TLS를 분석한 뒤, SET와의 장·단점을 비교/분석한다. 또한, SET 이후에 새롭게 등장한 3D SET와 3-D Secure, 그리고 Wireless SET의 동향을 분석한다.

본 고의 구성은 다음과 같다. 제 2장에서는 SET의 기능과 구성요소들을 살펴보고, SET에 사용된 보안기술 및 SET의 지불정보 흐름을 살펴본다. 또한, 전자상거래 초창기 때부터 사용되었던 SSL/TLS를 분석하고, SSL/TLS와 SET와의 장·단점을 비교/분석한다. 그리고 제 3장에서는 SSL/TLS와 SET의 장점을 모두 만족시키는 새로운 모델인 3D SET와 3-D Secure를 분석하고, PDA나 휴대폰과 같은 모바일 환경에서의 전자지불을 위한 Wireless SET에 대한 동향을 분석한다. 마지막으로 4장에서 결론을 맺는다.

II. SET(Secure Electronic Transaction)

본 장에서는 SET의 개요 및 기능적 요구사항, 구성요소 등을 살펴보고, SET에 사용된 보안기술과 지불정보 흐름에 대해서 살펴본다.

2.1 SET의 개요

SET는 Visa 카드사와 Master 카드사가 공동으로 제안하고, GTE, IBM, Microsoft, Netscape, SAIC, Terisa 그리고 Verisign 사 등의 기술지원하에 개발되어 Visa 카드사와 Master 카드사에 의해 1997년 5월에 발표된 신용카드 기반의 전자지불시스템 표준 프로토콜이다.[3-5]

SET는 현실세계의 신용카드 지불시스템을 기반으로 인터넷 전자상거래 환경을 실현하기 위해 전자상거래 요소 시스템간의 지급 및 인증시스템을 규정하고 있다.

2.2 SET의 기능적 요구사항

2.2.1 정보의 비밀성(Confidentiality)

인터넷을 통한 거래에서는 특정 사용자의 거래정보가 유출될 수 있는 위험이 존재한다. 이렇게 물품을 구매하는 사람의 신용카드 번호와 지불정보, 구매정보 등의 상거래 정보가 유출되면, 개인의 사생활이 침해받을 가능성이 높아진다. 따라서 SET에서는 비밀정보를 암호화하여 교환함으로써 정보의 기밀성을 유지한다.

2.2.2 데이터의 무결성(Integrity)

모든 거래에 있어서 지불정보가 전송 중에 위·변조되지 않았다는 것을 증명하기 위해 SET에서는 전자서명(Digital Signature)을 사용한다. 전자서명은 메시지의 무결성과 인증을 제공하기 위해서 공개키 암호화 알고리즘을 이용하여 서명하는 기법으로서, 해쉬함수와 공개키 암호를 사용하여 제공된다.

SET에서 두 명의 당사자는 보낸 메시지와 받은 메시지가 정확히 일치하는지를 확인함으로써 거래정보의 무결성을 제공한다.

2.2.3 구매자에 대한 인증(Authentication)

신용카드를 가지고 거래를 하는 구매자에 대한 인증은 구매자가 인증기관에서 발급받은 인증서와 전자서명을 사용하여 해당 구매자가 유효한 신용카드 사용자임을 확인한다.

2.2.4 판매자에 대한 인증

구매자의 입장에서 볼 때 자신이 거래하는 판매자가 해당 브랜드의 카드를 수용할 수 있는 권한을 지니고 있는지 확인하기 위해 전자서명과 함께 판매자가 인증기관에서 발급받은 인증서를 사용한다.

2.2.5 보안 기술의 적용

전자상거래의 모든 구성원을 보호하기 위해 효율적이면서도 강력한 보안성을 제공하기 위해 공개키 암호화 알고리즘과 관용 암호화 알고리즘 및 전자서명(Digital Signature), 전자봉투(Digital Envelope), 이중서명(Dual Signature)등의 보안 기술을 사용한다.

2.2.6 구현의 독립성 보장

기존 전자지불처리 기술과 달리 특정 벤더에 영향을 받지 않고 다양한 하드웨어와 소프트웨어에서 적용할 수 있는 구조로 설계되어 다양한 응용 소프트웨어의 개발이 가능하게 되었다.

2.3 SET의 구성

SET를 기반으로 하는 전자지불처리시스템은 카드 소지자가 사용하는 구매자 소프트웨어(Cardholder Software)와 판매자가 사용하는 판매자 서버시스템, 신용카드 발행사(Issuer)와 매입사(Acquirer)가 연동되기 위한 지불게이트웨이, 그리고 각 구성 요소들의 인증서를 발부해주는 인증 서버시스템(CA)으로 구성된다.

2.3.1 구매자 소프트웨어

구매자 소프트웨어는 SET 프로토콜을 처리하기 위한 일종의 전자지갑 소프트웨어로서, 지불처리시 판매자 서버에서 전송되는 구동 메시지에 의해 시작되는 것이 일반적이다. 구매자 소프트웨어는 구매자의 구매 및 지불정보의 보호, 인증서 및 개인키 관리, 거래 내역의 관리, 판매자 서버와 연동한 SET 전자지불처리를 주요 기능으로 한다.

2.3.2 판매자 서버시스템

판매자 서버는 구매자의 구매 요구 및 지불 명령을 처리한다. 주요 기능은 거래 정보의 보호 및 거래 내역을 관리하는 것이며, 판매자의 공개키 및 개인키를 관리, 고객의 주문 처리, 지불게이트웨이에 대한 인가, 요구 및 대금 이체 요구 등을 수용한다.

2.3.3 지불게이트웨이

지불게이트웨이는 일종의 지불 대행 시스템으로, 매입사(판매자와 계약을 체결하여, 카드결제에 대한 신뢰성과 지불을 담당하는 금융기관) 혹은 믿을 수 있는 제 3의 기관에서 운영될 수 있다. 지불게이트웨이의 주요 기능은 판매자로부터의 인가 메시지와 대금 이체 메시지를 매입사로 전송하여 처리하는 것이며, 그 외에도 거래 사고의 방지를 위한 거래내역 관리, 신용도에 따른 인증 서버의 인증서 취소 리스트와의 연동, 판매자 서버와의 연동 등을 수행한다.

2.3.4 인증 서버시스템

인증국에서 운영되는 인증 서버시스템은 SET 거래에 참가하는 구성 요소들에 대한 등록과 인증서 발행을 주요 목적으로 하고 있으며, 믿을 수 있는 기관에 의해 운영되는 방식이어야 한다. 인증 서버의 주요 기능은 인증서의 발행 및 관리를 비롯하여, 잘못된 인증서를 알리는 인증서 취소 리스트(CRL)의 운용, 은행망과 연동하여 고객 및 상인의 인증서 취소 또는 재발행, 다른 인증 서버와의 연동 등이 있다.

2.4 SET의 지불정보 흐름

2.4.1 SET의 전자쇼핑 시나리오

단계 1: 고객이 판매자의 웹 홈페이지에서 구매할 상품을 검색하고 선택한다.

단계 2: 선택된 상품에 대한 가격, 선적 요금 등을 포함한 구매정보(OI)를 판매자로부터 획득한다.

단계 3: 구매정보와 신용카드번호, 유효기간 등의 지불정보(PI)를 이중서명(DSc)하고, 지불정보에 관한 전자봉투(ENVp)를 생성하여 판매자에게 보낸다.

단계 4: 판매자는 구매정보와 이중서명을 확인한 후 암호화된 결제정보와 자신의 개인키로 전자서명된 승인요청 전문을 전자봉투 처리하여 지불게이트웨이로 전송한다.

단계 5: 지불게이트웨이는 판매자로부터 전송된 전자봉투 및 결제정보를 복호화한 후 정당한 결제요청인지를 확인한 뒤, 매입사와 연동하여 지불인가를 요청하고 그 결과를 판매자에게 전송한다.

단계 6: 판매자는 지불인가 결과에 따라 거래가 성립되었다면 구매확인서를 구매자에게 전송한다.

단계 7: 판매자는 성립된 거래에 대한 서비스를 수행한다.

단계 8: 판매자는 지불게이트웨이에 결재를 요구하고, 지불게이트웨이는 판매자가 전송한 결재 요구를 매입사와 연동하여 수행한다.[6,7]

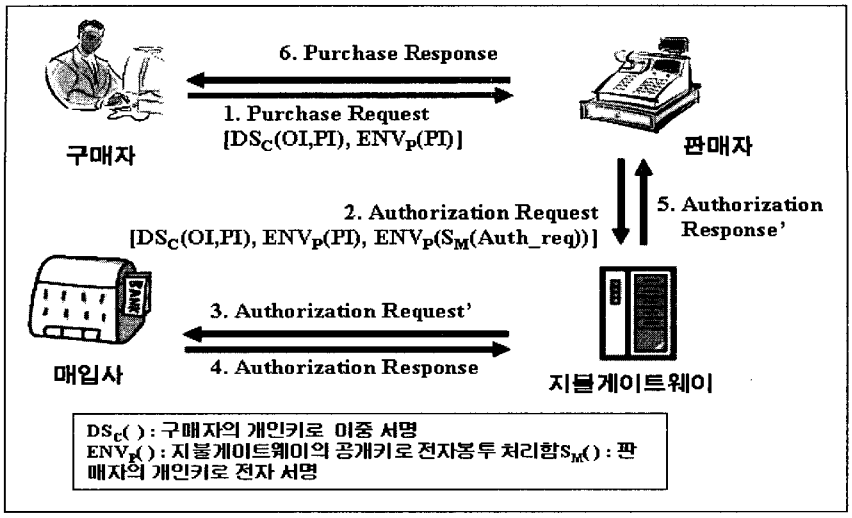
2.5 SET에 사용된 보안기술

2.5.1 전자서명(Digital signature)

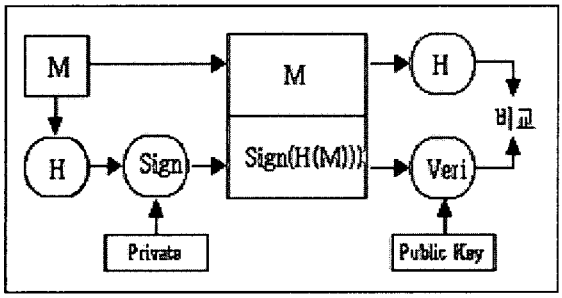
공개키 암호화 방식에서 개인키로 서명된 것은 이에 대응하는 유일한 공개키에 의해서만 검증될 수 있다. 이런 수학적 알고리즘의 특징은 전자서명에 이용될 수 있다. 그림 1은 기본적인 전자서명의 흐름을 나타내고 있다. 여기서 M은 메시지, H는 해쉬 알고리즘, Sign은 서명을, Veri 검증을 나타낸다. 메시지로부터 생성된 해쉬값에 서명한 값이 전달받은 메시지로부터 생성된 해쉬값과 같은지 비교하여 동일하면 사용자 인증과 서명 대상인 메시지에 대한 인증을 동시에 실시할 수 있다.[8,9]

2.5.2 전자봉투(Digital envelope)

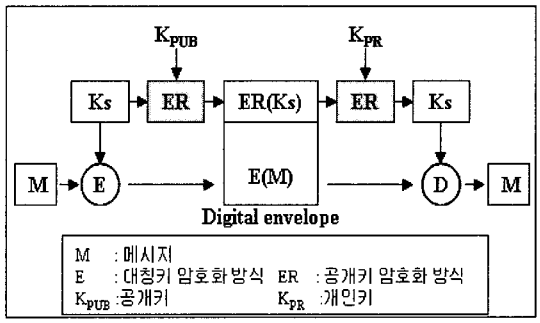
전자서명은 전송되는 메시지에 대한 기밀성을 제공하지 못한다. 전자봉투는 이를 해결하기 위한 방법으



〔그림 1〕 지불정보 흐름



〔그림 2〕 전자서명



〔그림 3〕 전자봉투

로 전자서명된 메시지를 관용 암호방식으로 암호화하고, 여기에 사용된 대칭키는 수신자의 공개키로 암호화해서 함께 전송하는 방식을 말한다. 전자서명에 의한 사용자 인증과 메시지에 대한 인증과 동시에 메시지에 기밀성을 제공할 수 있다.[8,10]

2.5.3 이중서명(Dual signature)

이중서명은 판매자에 대해서는 지불정보의 투명성을 매입자에 대해서는 구매정보의 투명성을 제공하기 위한 방법이다. 서로 다른 공개키로 암호화된 지불정보와 구매정보를 연결하여 지불정보의 실제 내용을 모르더라도 지불정보의 무결성을 검사할 수 있는 방법을 제공한다.[6-8]

① 이중서명 생성

식(1)에서 OI와 PI의 해쉬값을 연결하여 새로운 해쉬값 H_2를 생성하고 이것을 S_C로 전자서명 한다. $S_C(H_2)$와 H(OI)와 H(PI)의 XOR 연산된 값이 이중서명 $DS_C(OI,PI)$를 구성한다.

$$H_2 = H(\{H(OI), H(PI)\}) \quad (1)$$

$$S_2 = S_c(H_2) \quad (2)$$

$$DS_c(OI,PI) = \{S_2, (H(OI) \oplus H(PI))\} \quad (3)$$

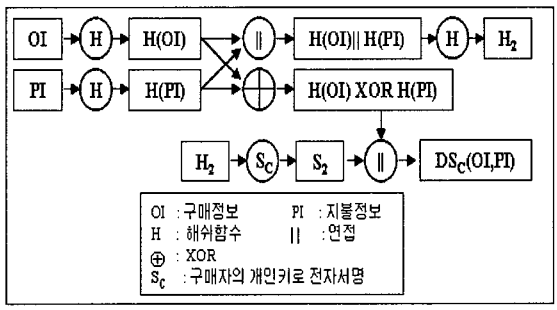


그림 4. 이중서명의 생성

② 판매자의 이중서명 확인

판매자는 자신이 가지고 있는 OI값에 대한 해쉬값 H_3을 식(4)와 같이 생성한다. 구매자로부터 전송받은 정보에서 판매자는 PI값을 복호화할 수 없다. 따라서 H(PI)값을 얻기 위해서는 $S_C(H_2)$로 전송된 정보를 식(5)와 같은 방법을 통하여 H(PI)를 얻을 수 있다. 식(6)을 통하여 H_2'값을 생성하고 이 값과 식(7)을 통해서 얻은 값과 비교하여 전송된 지불정보와 구매정보의 무결성을 확인한다.

$$H_3 = H(OI) \tag{4}$$

$$H_4 = (H(OI) \oplus (H(OI) \oplus H(PI))) \tag{5}$$

$$H_2' = H(\{H_3, H_4\}) \tag{6}$$

$$H_2 = D_c(S_2) \tag{7}$$

③ 지불게이트웨이의 이중서명 확인

판매자로부터 전송된 지불정보가 해당 구매정보와 관련된 유효한 정보인지 확인하기 위해 지불게이트웨이는 자신의 개인키로 판매자로부터 전송된 전자봉투처리된 지불정보를 해독하여 PI를 얻고 이에 대한 해쉬값을 식(8)과 같이 얻는다. 식(9)에 따라 H(OI)를 얻고 이를 H_5와 해쉬하여 H_2''를 얻는다. 얻어진 H_2''값과 H_2값을 비교하여 PI에 대한 해당 OI정보가 유효한지 판단한다.

$$H_5 = H(PI) \tag{8}$$

$$H_6 = H(PI) \oplus (H(OI) \oplus H(PI)) \tag{9}$$

$$H_2'' = H(\{H_5, H_6\}) \tag{10}$$

Ⅲ. SSL/TLS

본 장에서는 전자상거래 초창기 때부터 이용되었던 SSL/TLS를 분석하고, SSL/TLS와 SET과의 장·단점을 비교/분석한다.

3.1 SSL/TLS의 개요

SSL(Secure Socket Layer)은 1994년 Netscape사에서 웹 브라우저 보안을 위한 프로토콜로 처음 제안하였고, 1996년 IETF(Internet Engineering Task Force)는 이를 보완한 SSL 3.0을 제안하였다. 이후에도 SSL 3.0은 지속적으로 수정·보안되었으며 1999년에 TLS(Transparent Layer Security)로 명칭이 바뀌어 RFC 2246(TLS 1.0)으로 표준화되었다.[11]

SSL/TLS는 클라이언트-서버 환경에서 TCP상의 응용 프로토콜에 대한 종단간 보안을 제공하기 위해 고안된 전송계층 보안 프로토콜로 웹 브라우저와 웹 서버가 각각 클라이언트와 서버 역할을 한다. 대칭키 암호 방식(symmetric cryptosystem)을 이용한 암호화를 통해 기밀성(confidentiality)을 제공하고, 메시지 인증 코드(MAC : Message Authentication Code)를 사용하여 전송되는 데이터의 위/변조를 탐지할 수 있는 무결성(integrity) 서비스를 제공한다.

SSL/TLS는 인터넷 프로토콜의 TCP 계층과 HTTP나 LDAP, IMAP와 같은 응용계층 사이에서 동작한다. SSL/TLS는 신뢰할 수 있는 전송계층 프로토콜(reliable transport protocol) 위에서만 동작하도록 설계되었으므로 UDP 응용을 보호하는 데는 사용될 수 없다.

SSL/TLS는 기존의 통신 프로토콜과 독립적으로 두 계층 사이에 삽입되는 형태이기 때문에 SSL/TLS가 삽입되는 상/하위 계층의 프로토콜들에 대한 영향을 최소화할 수 있을 뿐만 아니라 TCP상의 다양한 응용 프로토콜들을 지원할 수 있다는 장점이 있다.

3.2 SSL/TLS 기반 전자지불시스템 시나리오

단계 1: 소비자와 판매자는 Hello 요청을 보내는 것으로 통신을 시작한다.

단계 2: 구매자와 판매자는 자신의 인증서를 보냄으로써 상호인증을 완성한다.

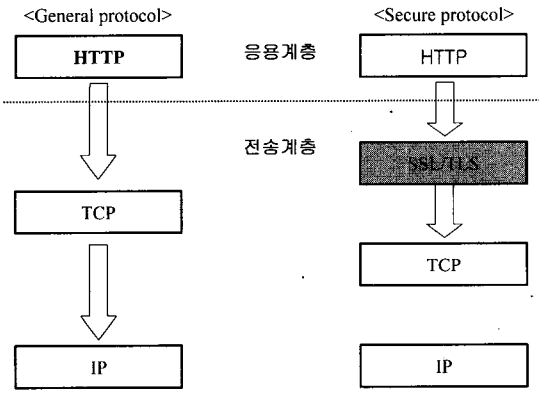
단계 3: 구매자는 세션키를 생성하고 이 세션키를 생성하는데 이용되는 비밀정보를 판매자의 공개키로 암호화하여 보낸다.

단계 4: 구매자는 상품검색을 끝마친 후 구입정보와 카드정보 등 중요한 정보를 자신의 세션키를 이용하여 암호화하여 판매자에게 보낸다.

단계 5: 판매자는 3단계의 비밀정보를 이용하여 세션키를 생성한 다음 구매자로부터 받은 데이터의 내용을 확인한다.

단계 6: 판매자는 구매자의 카드정보와 결제금액을 매입사에 보내서 결제를 받고 매입사로부터 영수증을 받는다.

단계 7: 판매자는 받은 영수증을 단계 5에서 생성한 세션키를 이용하여 암호화 한 다음 구매자에게 전송한다.[12]



〔그림 5〕 SSL/TLS 프로토콜의 위치

3.3 SSL/TLS와 SET의 장·단점

3.3.1 SSL/TLS의 장·단점

① 장점

- End-user들이 전자상거래를 이용하기에 편하다. SSL은 일반적으로 사용되는 웹 브라우저에 탑재되어 있기 때문에 구매자들은 그것을 쉽게 사용할 수 있고 판매자들 또한 지불모델을 바꾸지 않고도 SSL을 실행할 수 있다.
- 시스템이 복잡하지 않아 전송 속도에 영향을 거의 미치지 않는다.

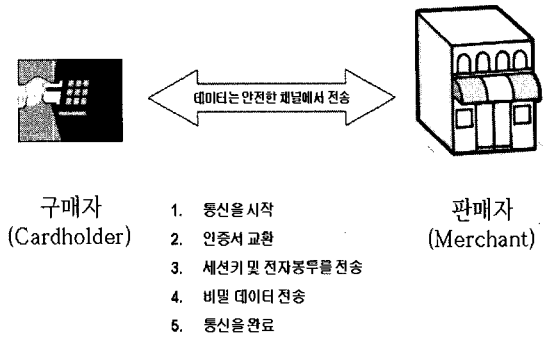
② 단점

- 판매자는 구매자의 신분을 신뢰할 수 없다는 것이다. 구매자가 훔친 신용카드를 이용하여 전자상거래를 했을 때 판매자는 분실된 카드를 이용한 거래에 대하여 책임져야 한다.
- SSL은 구매자와 판매자 사이의 통신연결만 보호해주기 때문에 판매자의 서버에 저장되어 있는 구매자의 중요한 정보는 아무런 보안조치가 되어 있지 않다. 따라서, 판매자는 추가적인 보안기술을 서버에 적용하여 중요한 정보를 보호하여야 한다.
- SSL 기반의 전자상거래에서 판매자들이 구매자의 지불정보를 볼 수 있기 때문에 구매자의 프라이버시에 대하여 잠재적인 위협이 될 수 있다.

3.3.2 SET의 장·단점

① 장점

- SET는 데이터 전송과 저장을 포함한 전송과정의 모든 단계에서 지불정보의 기밀성을 보장해준다.



〔그림 6〕 SSL/TLS 기반 전자지불시스템

- SET는 지불정보를 매입사의 공개키로 암호화하여 판매자에게 전송하기 때문에 판매자들이 구매자의 지불정보를 볼 수 없다.
- SET는 판매자의 프라이버시 보호를 위해서 매입사가 판매자의 웹 서버에 저장되어 있는 구매자의 상품정보를 볼 수 없도록 해준다.

② 단점

- SET 기반 전자상거래는 SSL 기반 전자상거래보다 비용이 많이 든다.
- SET는 SSL보다 사용이 복잡하다.
- 구매자는 SET가 초기화된 구매자 자신의 PC에서만 전자상거래를 할 수 있다. 그 이유는 SET를 실행하는데 필요한 구매자의 개인키가 자신의 PC에 저장되어 있기 때문이다.
- SET는 복잡한 암호화 알고리즘을 사용해서 전송속도가 엄청나게 느려진다.[12,13]

Ⅳ. 3D Security scheme

본 장에서는 SET 이후에 새롭게 등장한 3D Se-

〔표 1〕 SSL/TLS와 SET의 장·단점 비교

	장 점	단 점
SSL/TLS	- 사용 편의성 - 빠른 전송속도	- 구매자에 대한 인증 메커니즘의 부재 - 판매자 서버의 노출로 인한 구매자의 중요한 정보 노출 - 판매자에게 구매자의 지불정보가 노출
SET	- 판매자로부터 구매자의 지불정보를 보호 - 매입사로부터 구매자의 상품정보를 보호	- 고비용 - 사용상의 불편 - 느린 전송속도

curity scheme에 대해 살펴본다. 먼저, 3D Security scheme의 도메인 구성을 살펴보고, 3D Security scheme인 3D SET와 3-D Secure에 대해 분석한다.

4.1 3D Security scheme의 도메인 구성

3D SET와 3-D Secure는 3개의 도메인으로 구성된다. 첫째로, 판매자와 매입사 사이의 통신이 이루어지는 매입사 도메인, 구매자와 신용카드 발생사 사이의 통신이 이루어지는 카드 발행사 도메인, 매입사 도메인과 카드 발생사 도메인 간의 통신이 이루어지는 상호운영 도메인으로 구성된다.[13]

4.2 3D SET

3D SET는 기존의 SET 시스템에 3D 모델을 추가한 시스템이다. SET 전자지갑이 구매자의 PC에 저장되는 기존의 SET와는 달리, 3D SET는 카드 발행사 도메인에 SET 전자지갑 서버를 추가하였다. 구매자의 인증서 역시 신용카드 발행사의 비밀서버에 안전하게 저장된다. 카드 발행사 도메인과 마찬가지로 매입사 도메인에서도 매입사의 비밀서버에 지불게이트웨이를 설치하고, 판매자의 인증서는 매입사에 저장된다.[14]

4.2.1 3D SET의 동작과정

단계 1: 구매자는 판매자에게 거래요청 메시지(SR : SET Request)를 보낸다.

단계 2: 판매자는 요청에 대한 응답(SW : SET Wake-up) 메시지를 보낸다.

단계 3: 구매자의 PC에서 동작 중인 브라우저는 판매자에게서 받은 SW 메시지를 신용카드 발행사측의 Wallet Server에게 전달한다.

단계 4: 신용카드 발행사는 구매자에게 결제정보(PI : Payment Information)를 보여주고, 구매자의 신분을 확인할 수 있는 인증 정보(SAR : Secret Authentication Information)를 요청한다.

단계 5: 구매자는 인증 정보(SA)를 신용카드 발행사에게 보내고, 신용카드 발행사에 의해 올바른 사용자임이 확인되면 SET 통신이 시작된다.

단계 6: 판매자에게 성공적으로 인증이 종료되었다는 것을 알려준다.

단계 7: 판매자는 지불인가 요청(PAR : Payment Authorization Request)을 매입사에게 보낸다.

단계 8: 매입사는 지불인가 요청(PAR)을 신용카드 발행사에게 전달한다.

단계 9: 지불인가 요청(PAR)을 받은 신용카드 발행사는 카드 사용가능 여부를 확인한 후 지불 허가(PA : Payment Authorization)메시지를 매입사에게 보낸다.

단계10: 매입사는 지불허가(PA)메시지를 확인한 후 판매자에게 전송한다.

단계11: 지불허가(PA)메시지를 확인한 판매자는 구매자에게 구매물품에 대한 영수증을 발급해 준다.

4.3 3-D Secure

3-D Secure는 SSL과 3D(three-domain) 모델이 결합된 지불시스템으로, 인증시스템의 부재와 판매자로부터 구매자의 지불정보가 노출되는 SSL/TLS의 문제점을 보완하였다.

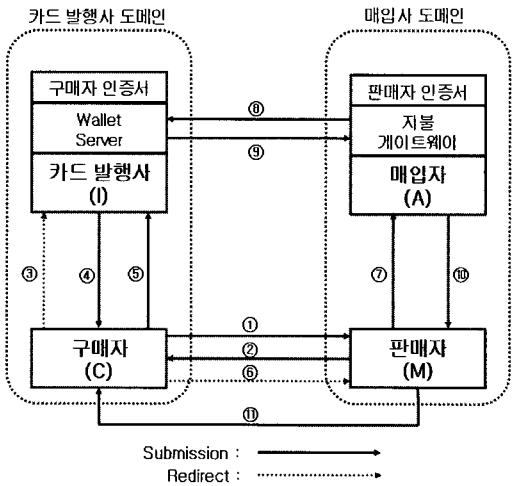
4.3.1 3-D Secure에 추가된 구성요소

① VisaNet

Visa사가 소유하고 있는 지불 네트워크를 의미한다.

② MPI(Merchant Plug-In)

판매자 서버 내에 위치해 있으며, 구매자와 판매자 사이의 비밀통신을 위해 SSL/TLS가 포함된 소프트웨어이다.



〔그림 7〕 3D SET의 동작과정

③ ACS(Access Control Server)

신용카드 발행사 서버 내에 위치하며, 구매자의 인증을 담당하는 서버이다.

④ Visa Directory

판매자 서버와 신용카드 발행사 간의 통신을 담당하는 서버이다.

4.3.2 3-D Secure의 동작과정

3-D Secure에서는 각 개체들 사이에서 발생하는 통신의 보안을 위해 구매자-판매자, 구매자-ACS, 판매자-Visa Directory, 그리고 Visa Directory-ACS 사이의 링크는 SSL/TLS를 사용하고 있다.[15-17]

단계 1: 구매자는 구매결정을 마친 후에 판매자에게 결제요청(CR : Checkout Request)을 한다. 이때, 판매자 서버로 전송되는 모든 구매정보는 SSL/TLS에 의해서 보호된다.

단계 2: 구매정보를 받은 후, 판매자 서버 내에 있는 MPI는 신용카드 발행사측에 있는 ACS의 URL을 Visa directory에게 요청한다.

단계 3: Visa Directory는 신용카드 발행사 서버 내의 ACS에게 카드사용 가능여부를 요청한다.

단계 4: 신용카드 발행사는 카드사용 가능여부에 대한 결과를 포함하고 있는 확인 메시지(CM : Confirmation Message)를 Visa Directory에게 보내준다.

단계 5: Visa Direction은 신용카드 발행사로부터 받은 ACS의 URL을 MPI에게 보내준다.

단계 6: MPI는 구매자의 브라우저가 신용카드 발행사의 ACS로 향하도록 해준다.

단계 7: 신용카드 발행사의 ACS는 구매자에게 사용자 이름이나 패스워드 등의 비밀인증(SA : Secret Authentication) 정보를 요청한다.

단계 8: 구매자는 비밀인증(SA)정보를 ACS에게 보내준다.

단계 9: 구매자에 대한 인증과정이 종료되면, ACS는 구매자의 브라우저가 다시 MPI와 통신할 수 있도록 한 후, 신용카드 발행사에 의해 확인된 지불확인 메시지를 판매자에게 보낸다.

단계10: 판매자는 매입사에게 자세한 금액 내역을 보내주고, 지불허가(PA)를 요청한다.

단계11: 매입사는 지불허가요청을 Visa Net을 경유하여 신용카드 발행사에게 보낸다.

단계12: 신용카드 발행사는 지불허가(PA)메시지를 매입사에게 보낸다.

단계13: 매입사는 지불허가(PA)메시지를 판매자에게 보낸다.

단계14: 판매자는 지불허가(PA)메시지를 확인하고 구매자에게 영수증을 발급한다.

4.3.3 3D SET와 3-D Secure의 비교

최종 사용자의 요구사항에 따라 3D SET와 3-D Secure를 비교할 수 있다. 여기서는 각 요구사항에 대해 간단히 살펴보겠다.

3D SET와 3-D Secure는 e-commerce에서 가장 중요한 요건인 최종 사용자의 보안 요구사항을 모

〔표 2〕 최종 사용자 요구사항

보안 요구사항	
Confidentiality	고객의 금융 정보는 타인이 볼 수 없도록 안전하게 저장되어야 한다.
Integrity	데이터는 전송되거나 저장되는 도중 값이 변하지 않아야 한다.
Authentication	각 개체는 거래하고 있는 상대방에 대한 인증이 가능해야 한다.
Non-repudiation	트렌젝션에 참가하는 모든 개체들은 자신이 수행한 결과에 대한 부인은 불가능하다.
구현 요구사항	
Usability	사용자가 쉽게 사용할 수 있어야 한다.
Flexibility	사용자는 PC뿐만 아니라 다른 기기를 통해서도 서비스를 제공받을 수 있어야 한다.
Affordability	시스템 구현과 사용 비용을 사용자가 감당할 수 있어야 한다.
Reliability	시스템은 신뢰성 있는 서비스를 제공해야 한다.
Availability	시스템은 필요한 서비스를 제공할 수 있어야 한다.
Speed of transaction	처리 속도가 적정 수준을 유지하여야 한다.
Interoperability	다른 플랫폼의 기기들에서도 동작하여야 한다.

두 만족시킨다. 3D SET와 3-D Secure는 지불 정보를 암호화해서 상대방에게 보내기 때문에 지불 정보에 대한 confidentiality를 만족하며, 지불 정보에 대한 서명이 이루어진 후 네트워크를 통해 전송되기 때문에 전송된 정보에 대한 integrity 역시 만족한다. 3D SET에서는 카드 발행사가 구매자에 대한 인증을, 매입사가 판매자에 대한 인증을 수행하고, 3-D Secure에서는 ACS를 통해 구매자에 대한 인증이 이루어지기 때문에 authentication과 non-repudiation 또한 만족한다.

3D SET와 3-D Secure 모두 보안 요구사항을 만족하는 반면, 구현 요구사항 측면에서는 3-D Secure가 훨씬 나은 성능을 보인다. 3-D Secure에서 판매자는 자신의 서버에 간단한 plug-in 소프트웨어를 설치하고, 구매자는 추가의 소프트웨어 설치 없이 기존의 SSL/TLS를 사용함으로써 안전한 통신을 할 수 있지만, 3D SET의 경우 현재의 시스템에서 3D SET를 사용하기 위해서는 구매자와 판매자의 PC에 따로 소프트웨어를 설치해야 하는 등 3-D Secure에 비해 추가로 드는 비용이 증가하므로 usability와 affordability, availability 측면에서 3-D Secure가 더 나은 효과를 보인다.

V. WSET(Wireless SET)

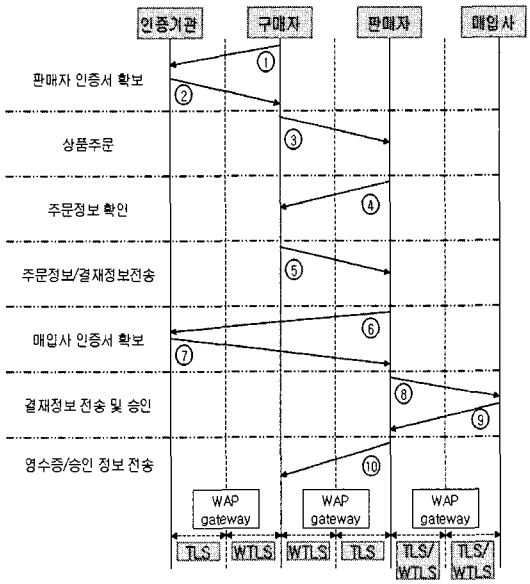
본 장에서는 모바일 환경에서의 전자지불을 위한 Wireless SET의 개요와 동작과정에 대해 살펴본다.

5.1 WSET의 개요

WSET는 WAP 기반의 M-commerce를 위한 전자지불시스템으로, 보안서비스를 강화시키기 위해서 TLS/WTLS와 SET를 결합하였다. 다시 말하면, WSET는 유선 인터넷의 공간 제약성이라는 한계를 극복하고 나날이 다양하게 변화하는 소비자들의 욕구를 반영하며, 더 빠르면서 이동성까지 요구하는 시장에 적용 가능한 무선인터넷 전자상거래 결제시스템이다.[18]

5.2 WSET의 동작과정

단계 1: 구매자가 모바일 인터넷으로 상품을 구입하고자 할 때, 우선 판매자의 인증기관에 등록여부를 확인하여야 한다. 이를 위하여 구매자는 자신의 정보, 판매자의 정보, 구매자 자신의 정보와 판매자의 정보를 자신의 개인키 로 암호화하고, 이 모든 내용을



(그림 8) WSET의 동작과정

인증기관의 공개키로 다시 암호화하여 인증기관에게 전송한다.

단계 2: 인증기관은 판매자를 인증하는 인증기관의 유효기간과 판매자의 ID, 공개키, 인증서를 구매자의 공개키로 암호화한 후 구매자에게 전송한다.

단계 3: 구매자는 상품 주문 메시지와 구매자 자신의 인증서를 판매자의 공개키로 암호화하여 판매자에게 전송한다.

단계 4: 판매자는 상품 주문 메시지, 지불 요구 메시지, 상품 주문 메시지와 지불 요구 메시지를 판매자의 개인키로 암호화한 후, 이 모든 내용을 구매자의 공개키로 다시 암호화하여 구매자에게 전송한다.

단계 5: 구매자는 판매자에 대한 구매 지불 요구서의 이중서명 정보, 매입사에 대한 구매 지불 요구서의 이중서명 정보를 구매자와 매입사의 공통키를 이용하여 암호화한 후, 이 모든 내용 판매자의 공개키로 암호화하여 판매자에게 전송한다. 판매자는 자신의 개인키로 암호문을 복호화한 후 확인하고, 매입사의 공개키로 암호화된 정보는 단계 8에서 매입사에 보낼 정보이므로 잠시 저장해 둔다.

단계 6: 판매자는 지불게이트웨이를 운영하는 매입사가 인증기관에 등록이 되어 있는지 확인

하기 위해 판매자의 정보, 은행 정보, 판매자와 은행의 정보를 판매자의 개인키로 암호화한 후 이 모든 내용을 인증기관의 공개키로 다시 암호화하여 인증기관에 전송한다.

단계 7: 인증기관은 매입사의 인증유효기간, ID, 공개키를 판매자만이 알 수 있도록 이 모든 내용을 판매자의 공개키로 암호화하여 판매자에게 전송한다.

단계 8: 판매자는 판매자의 인증유효기간, ID, 공개키, 인증서와 구매자의 인증서, 단계 5에서 저장해둔 정보를 매입사의 공개키로 모두 암호화하여 매입사에게 전송한다.

단계 9: 매입사는 판매자에게 결재가 승인되었음을 알리는 메시지와 판매자에게 결재가 승인되었음을 알리기 위한 메시지를 매입사의 개인키로 암호화하여 판매자에게 전송한다. 그리고 구매자에게 전달될 결재승인정보를 구매자와 매입사와의 비밀키로 암호화한 후, 이 모든 내용을 판매자의 공개키로 다시 암호화하여 판매자에게 전송한다.

단계10: 판매자는 영수증, 판매자의 전자서명, 구매자에게 주는 결재승인정보를 구매자와 매입사의 비밀키로 암호화한 후, 이 모든 내용을 구매자의 공개키로 다시 암호화하여 구매자에게 전송한다.

Ⅵ. 결 론

본 고에서는 SET의 기능과 구성요소들을 살펴보았으며, SET에 사용된 보안기술 및 SET의 지불정보 흐름에 대해서 살펴보았다. 또한, 전자상거래 초창기 때부터 사용되었던 SSL/TLS를 분석한 뒤, SSL/TLS와 SET와의 장·단점을 비교/분석하였다. 그리고 SET 이후에 등장한 새로운 모델인 3D SET와 3-D Secure에 대해서 분석하였으며, 모바일 환경에서의 전자지불을 위한 WSET에 대해서도 살펴보았다.

참 고 문 헌

[1] K.E.B. Hickman, "Secure Socket Library", Netscape Communications, 1994

[2] E. Rescorla, A.Schiffman, The Secure HyperText Transfer Protocol, Internet Draft, Enterprise Integration Technologies, December, 1994

[3] MasterCard and VISA, "Secure Electronic Transaction(SET) Specification", Book 1: Business Description(draft for testing), June, 1996

[4] MasterCard and VISA, "Secure Electronic Transaction(SET) Specification", Book 2: Programmer's Guide(draft for testing), June, 1996

[5] MasterCard and VISA, "Secure Electronic Transaction(SET) Specification", Book 3: Formal Protocol Definition (draft for testing), June, 1996

[6] Jin_Jang Hwang, Sue-Chen Hsueh, Greater protection for credit card holders : a revised SET protocol", Computer Standards and Interfaces, pp.1-8, 1998

[7] Jin-Jang Hwang, Tzu-Chang Yeh, Jung-bin Li, "Securing on-line credit card payments without disclosing privacy information", Computer Standards and Interfaces, pp. 119-129, 2003

[8] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Inc, 1997

[9] 원동호, "현대암호학", 도서출판 그린, 2003

[10] D. Chaum, "Blind Signatures for Untraceable Payments", Advances in Cryptology Crypto82, Plenum Press, pp. 199-203, 1983

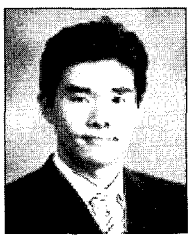
[11] T. Dierks and C. Allen, "The TLS Protocol version 1.0" IETF RFC 2246, January 1999

[12] P. Jarupunphol and C. J. Mitchell, "Measuring SSL and SET against e-commerce consumer requirements", In Proceedings of the International Network Conference, INC, pp. 323-330, 2002

[13] P. Jarupunphol and C. J. Mitchell, "Measuring 3-D Secure and 3D SET against e-commerce end-user requirements", In Proceedings of the 8th Collaborative electronic commerce technology and research conference, CollEC-

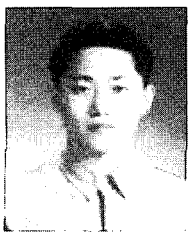
TeR (Europe), pp. 51-64, 2003
[14] J.J. Hwang, T.C. Yeh, and J.B. Li, "Securing on-line credit card payments without disclosing privacy information", Computer Standards and Interfaces 25, pp. 119-129, 2003
[15] Visa International, "3-D Secure: Introduction", Version 1.0.2, September, 2002
[16] Visa International, "3-D Secure: System Overview", Version 1.0.2, September, 2002
[17] Konrad Wrona, Marko Schuba, and Guido Zavagli, "Mobile Payments-State of the Art and Open Problems", L. Fiege, G. Muhl, and U. Wilhelm(Eds.), Proceedings of 2nd International Workshop WELCOM, voiume 2232 of LNCS, pp.88-200, 2001
[18] Alia Fourati, Hella Kaffel Ben Ayed, "A SET Based Approach to Secure the Payment in Mobile Commerce", Proceedings of the 27th Annual IEEE Conference on Local Computer Networks, LCN, 2002

〈著 者 紹 介〉



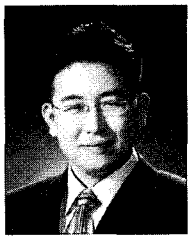
장 우 석 (Woosuk Chang)
학생회원

2005년 2월 : 건국대학교 소프트웨어학과 졸업(공학사)
2005년 3월~현재 : 성균관대학교 컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 네트워크 보안, 암호 프로토콜, DRM



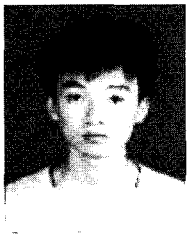
이 광 우 (Kwangwoo Lee)
학생회원

2005년 2월 : 성균관대학교 정보통신공학부 졸업(공학사)
2005년 3월~현재 : 성균관대학교 컴퓨터공학과 석사과정
〈관심분야〉 암호이론, 정보보호, 네트워크 보안, 전자투표, 워터마킹



최 동 현 (Donghyun Choi)
학생회원

2005년 8월 : 성균관대학교 정보통신공학부 졸업(공학사)
2005년 9월~ : 성균관대학교 컴퓨터공학과 석사과정
〈관심분야〉 암호이론, 정보보호, 네트워크 보안, DRM, 워터마킹



정 학 (Hak Chong)
학생회원

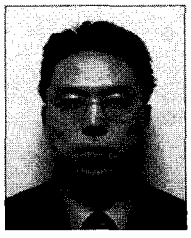
2004년 7월 : 연변 과학기술대학 컴퓨터공학과 졸업(공학사)
2005년 3월~현재 : 성균관대학교 대학원 컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 네트워크 보안

이 병 희 (Byunghee Lee)
학생회원

2005년 2월 : 성균관대학교 정보통신공학부 졸업(공학사)
2005년 3월~현재 : 성균관대학교 컴퓨터공학과 석사과정
〈관심분야〉 정보보안, 네트워크 보안, 해킹

최 윤 성 (Younsung Choi)
학생회원

2005년 현재 : 성균관대학교 정보통신공학부 학부재학
〈관심분야〉 암호이론, 정보보호, 네트워크 보안, 포렌식



김 승 주 (Seungjoo Kim)
종신회원

1994년 2월~1999년 2월 : 성균관대학교 정보공학과(학사, 석사, 박사)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장

2004년 3월~현재 : 성균관대학교 정보통신공학부 교수
2001년 1월~현재 : 한국정보보호학회 , 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 6월~현재 : 교육인적자원부 유해정보차단 자문위원
〈관심분야〉 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호 (Dongho Won)
종신회원

1976년~1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~2003년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, (정통부지정 ITRC)정보보호인증기술연구센터 센터장
〈관심분야〉 암호이론, 정보이론, 정보보호