신용카드 기반 전자지불시스템 분석

강성우, 박해룡, 천동현, 이재일
한국정보보호진흥원 암호인증기술팀

Study on the credit Payment Systems

Sungwoo Kang, Haeryong Park, Donghyun Cheon, Jaeil Lee
Electronic Transaction Security & Data Protection Division, KISA

요 약

전자상거래에서 신용카드를 이용하여 물품 대금을 지급하는 대표적인 방식으로 SSL과 SET을 사용하고 있다. 그러나, SSL은 시장의 폭넓은 지지를 받고 있지만, 카드소유자 본인 확인 기능이 없어서 카드소유자의 지불거부 뿐만 아니라, 부정거래가 발생할 수 있는 단점이 있다. 또한, SET도 카드소유자 본인 확인 기능이 없고 기술적으로 복잡해 시장의 큰 호응을 받지 못하는 단점이 있다. 이러한 SSL과 SET의 단점을 극복하기 위해서 최근 3D-SET, 3-D Secure가 개발되었으며, 3-D Secure 향후 신용카드 기반 전자지불시스템에서 주로 사용될 것으로 기대된다. 이에 본 논문에서는 3D-SET, 3-D Secure의 개요, 객체별 역할과 책임, 장점/단점 등을 비교 분석하고자 한다.

1. 서론

인터넷상에서 지불에 대한 시스템 개발을 억제한 주요 요인은 쉽게 구현되고 동시에 개방된 네트워크상에서 안전한 지불 시스템의 표준의 부재라고 할 수 있다. 신용카드를 이용한 전자거래에서 사용되는 안전한 전자지불 시스템으로 SSL에 기반한 방식과 SET이 가장 대표적인 방식이다. 그러나, 시장의 폭넓은 지지를 받고 있는 SSL 기반 방식은 전송되는 데이터를 보호하지만, 카드소유자 본인 확인 기능이 없다는 단점이 있으며, VISA사와 MasterCard사가 개발한 SET은 상점에게 개인 정보가 노출되지 않는 장점은 있지만 기술적으로 복잡해 시장의 큰 호응을 받지 못하고 외면당하고 있는 실정이다. 있다. 특히, MasterCard사의 전자거래의 80~85%가량이 카드소유자의 구매 부인으로 인한 지불거부라는 점은 카드소유자 인증의 필요성이 제기되었다. 주요 카드사들은 인터넷 거래에서 야기되는 지불거부 비율을 감소시키고, SET 시스템의 복잡성을 개선하기 위해 VISA사와 MasterCard사가 공동으로 SET에 카드소유자 인증 부분을 보완한 3D-SET, VISA사의 3-D Secure 각각 개발되었다. 이런 프로토콜들의 장점은 기존의 전자지불시스템이 제공하지 못했던 카드소유자 인증이 추가됨은 물론, 그로 인해 발행사가 카드소유자의 지불거부에 대한 책임을 지게 됨으로 책임 규명이 명확하게 이루어지게 된다. 특히, 3-D Secure는 발행사가 카드소유자를 인증했다는 증거를 상점에게 제공하고 카드소유자에게 영향을 최소화하였다.

본 문서에서는 위 문서를 바탕으로 3D-SET, 3-D Secure의 개요, 객체별 역할과 책임, 장점/단점 등을 서술하고자 한다.

2. 신용카드 기반 전자지불 시스템 분석

본 장에서는 신용카드 기반 전자지불시스템 3D-SET, 3-D Secure을 소개한다. 이러한 시스템이 안전성의 측면에서 기존의 SSL 기반 전자지불이나 SET에 비해서 개선된 점과 전자지불시스템의 실제적인 이용측면에서 기본 원칙인 구현의 용이성, 사용자가 어떤 상황에서 항상 이용가능 한지, 다양한 채널에 적용가능한지에 초점을 맞추어 각 시스템의 장점과 단점, 각 시스템 특성의 비교, 달라진 각 구성 객체의 역할과 책임에 대해 서술하겠다.

각 시스템의 소개에 앞서 본 문서에서 언급되는 신용카드 전자지불시스템 3D-SET, 3-D Secure의 기반이 되는 모델로써 기존 전자지불시스템과 차별화를

시켜주는 Three domain model의 개념을 살펴보겠다. 이 개념은 누가 무엇을 해야 하는지를 명확하게 규정하지 못했던 신용카드 거래 프레임 워크의 단점을 보완하기 위해 신용카드 거래 영역을 발행사 영역, 매입사 영역, 상호운영성 영역의 세 영역으로 구분하고 각 참가자들이 자신이 있는 위치가 어느 곳인가를 보여줌으로써 참가자들의 역할 및 의무 관계를 명확하게 구분하였다. 발행사 영역은 카드 소유자와 발행사 사이의 관계와 역할을 규정하는 영역으로 발행사가 카드소지자를 인증하는 과정이 수행되며 이에 따른 분쟁의 책임은 발행사가 지게 된다. 매입사 영역은 상점와 매입사 사이의 관계와 역할을 규정하고 있으며, 상호운영성 영역은 거래를 위해 인터넷(예: VisaNet)을 통해 수행되는 과정을 규정하고 있다.

가. 3D-SET

3D-SET은 VISA사와 MasterCard사가 개발한 SET(Secure Electronic Transaction)에 Three domain 개념을 도입한 것으로 VISA사에 의해 개발되어 1999년에 Visa International Board의 승인을 받아 2000년 5월 발행되었다. 3D-SET은 SET이 시장에서 받아들여지지 못하고 사장된 원인인 재정적인 이기의 부족, 세계적인 마케팅의 부족, 구현의 복잡성, Wallet과 인증서를 사용자 PC에 설치하는 것으로 인한 이동성(mobility)의 부족, 미국 시장의 지지 부족 등을 극복·보완하기 위한 시도라고 할 수 있다. 3D-SET은 Three domain model에 기반하고 있으며 3D-SET의 상호운영성 영역에서 일어나는 거래의 흐름도는 SET의 경우와 동일하다.

먼저, 안전성의 측면을 살펴보면, 3D-SET은 SET과 마찬가지로 이중 서명과 인증서를 이용하여 카드소유자와 상점사이의 인증, 거래의 무결성, 지불정보의 기밀성을 제공하고 있다. 특히, 사용자의 개인 정보가 상점에게 노출되지 않는다는 SET의 장점은 3D-SET도 그대로 가지고 있다. 다만, SET과 구별되는 안전성은 발행사가 선택한 인증 메카니즘을 통한 카드소유자 인증에 있다.

또한, 3D-SET이 SET보다는 구현이 용이하다. 왜냐하면, Sever Wallet은 발행사가 관리하고 카드소유자의 PC에는 큰 용량의 Wallet이 설치되지 않도록 설계하였기 때문이다. 상점의 SET POS Server는 매입사가 관리한다. SET과 3D-SET은 모두 카드소유자가 인증서를 가지고 등록하고 카드소유자의 PC에 부가적인 프로그램을 설치해야 하지만, SET에서 설치되는 Wallet program의 크기는 4Mb 정도이고, 3D-SET에서 설치되는 Thin Wallet은 100Kb 정도이다. Server Wallet의 구현의 경우는 mobile phone이나 set top box 등과 같은 authentication device에 쉽게 적용될 수 있다. 3D-SET은 SET의 개선된 버전이므로 SET에서 이미 이루어진 투자들을 그대로 유지할 수 있다. 특히, EMV 같은 chip 기술 등에 적용이 가능하다는 장점이 있다.

객체	역할과 책임
상점	- SET POS Server의 구현 - 카드소유자와 매입사의 Payment Gateway사이의 SET 거래 수행
매입사	- CA를 구축 - SET Payment Gateway 구현 및 인증서 적용
발행사	- SET Server Wallet 구현 - 카드소유자 인증을 위한 메카니즘의 선택 및 구현
카드소유자	- 카드소유자의 PC에서 Thin Wallet 구현
상호운영성 영역	-승인된 CA 이용(issuance of SET certificate) - Payment Scheme Network(authorization request and responses) 설정

[표 1] 3D-SET의 객체별 역할과 책임 비교표

다음 표는 SET 시스템과 3D-SET의 안전성 및 효율성에 대한 비교 분석을 나타낸 것이다.

성질	SET	3D-SET
안전성	- 카드소유자의 인증이 이루어지지 않음	- 카드소유자 인증이 발행사가 선택하는 인증 메카니즘에 의존하여 이루어짐
구현	- 구현이 복잡 SET은 (Thick) Wallet을 카드소유자의 PC에 설치해야 함	- SET 보다 구현이 용이 발행사가 Server Wallet을 동작시키고 카드소지자는 자신의 PC에 Thin Wallet을 설치하면 됨
적용성	- 다양한 채널에 적용하기 어려움	- mobile phone, PDA, set top box 등의 device를 이용하는 인증 채널에 적용이 용이함.
기타		- 상점은 매입사가 관리하는 SET POS Server를 선택할 수 있음

[표 2] SET와 3D-SET의 비교표

나. 3-D Secure

3-D Secure는 SET과 3D-SET 보다 간단하고 쉽게 적용할 수 있도록 VISA사에서 개발된 전자 지불 시스템이다. 3-D Secure는 client와 server 인증을 하는 SSL을 이용하여 개발되었다. VISA는 2002년 7월에 VISA 브랜드로만 사용할 수 있도록 3-D Secure를 개발하였으나, 2003년 3월에 VISA가 아닌 다른 브랜드로도 3-D Secure를 사용할 수 있도록 하기 위해 [2]에서 VISA 브랜드를 삭제하였다.

3D-Secure에서 발행사는 카드소유자를 등록하고 그것을 ACS(Access Control Server)에 등록을 하고, 구매 시 발행사의 책임 하에 ACS에서 선택된 인증 메카니즘을 이용하여 카드소유자를 인증을 수행한다. 상점는 구성요소인 MPI(Merchant Server Plug-in)를 적용해야 한다. 상점가 지불 거래 메시지를 받으면, MPI는 동작하고 카드소유자가 합법적인 등록자인지를 찾기 위해 VISA Directory를 통해 ACS에게 query를 보낸다. 만일 합법적인 등록자라면, MPI는 초기화되고 카드소유자 browser를 통해 ACS와 카드소유자 사이의 인증이 이루어지게 된다. 카드소유자에 대한 ACS의 인증 결과는 카드소유자의 browser를 통해서 서명된 응답으로 MPI에 전달된다. MPI는 ACS로부터의 응답을 체크하고, 매입사와 네트워크(e.g., VISANet)을 통해 승인 허가를 요청한다.

안전성 측면에서, 3-D Secure는 카드소유자를 포함하는 연동을 제외하고는 3-D Secure 메시지를 전달하는 모든 공개 네트워크 연동에서 상호 인증을 하기 위해 SSL/TLS를 사용하도록 요구된다. MPI와 DS, DS와 ACS 사이의 SSL 연동의 보호를 위한 요구사항은 지불 스킴(Payment Scheme) 적용에 의존된다.

- Acquiring : MPI와 DS 사이의 SSL 연동
  · DS는 공개적으로 발행된 server 인증서를 갖고 있다.
  · 상점은 상호 인증을 위해 SSL 지불 스킴에 의해서 발행된 client 인증서를 갖고 있다. 카드 스킴(e.g., VISA)는 SSL로 연결되고 DS에 등록된 상점 ID와 패스워드의 사용을 허용한다.
- Issuing : DS와 ACS 사이의 SSL 연동
  · DS는 지불 스킴에 의해 발행된 client 인증서를 갖고 있다.
  · ACS는 지불 스킴이나 공개 CA에 의해서 발행되는 server 인증서를 필요로 한다.

모든 카드 스킴(e.g., VISA)의 server와 client-server 사이의 인증과 ACS로부터 상점으로 서명 거래를 하는데 SSL을 기반으로 한다. 그리고 논쟁을 해결하기 위해 카드 스킴(e.g., VISA)는는 Authentication History server를 갖고 있다. 효율적인 측면에서, 카드 스킴(e.g., VISA)는 Directory와 History server가 모든 거래에 연관되므로 3D-SET보다 더 많이 관여한다. 그러나, 카드소유자 인증서는 없으며, 모든 server는 카드 스킴(e.g., VISA)에서 발행된 SSL 인증서만 적용하면 된다.

3-D Secure의 메시지 흐름은 다음과 같은 과정을 통해 이루어진다.

(1) 접속: 카드소유자는 상점의 홈페이지에 접속한다.
(2) Query 전송: MPI는 카드소유자 참여에 대한 체크를 하기 위해 Directory Server에 Query를 보낸다.
(3) Query 전송: Directory Server는 카드번호가 유효 카드 영역에 있는지 체크하고, 발행사의 ACS에 Query를 요청하고 발행사의 URL을 요청한다.
(4) 응답: ACS는 카드소유자가 ACS에 등록되었는지 체크하고, Directory Server를 통해 MPI에 응답을 보낸다.
(5) 인증 요청: MPI는 카드소유자의 browser를 통해 ACS에 인증 요청을 한다.
(6) 카드소유자 인증: ACS는 발행사에 의해서 선택된 보안 메카니즘을 통해 카드소유자를 인증한다.
(7) 인증 결과 저장 및 전송: 카드소유자 인증 결과는 카드소유자 browser를 통해 MPI에 서명되어 보내지고, 발생될 논쟁에 대비하여 서명된 결과를 Authentication History server 에 보내진다.
(8) 인증 요청: 상점 Server는 인증 요청을 매입사 Payment Gateway에 보낸다.
(9) 인증 요청: PG는 네트워크(e.g., VisaNet)를 통해 발행사에게 인증 요청을 한다.
(10) 인증 응답: 인증 응답은 발행사로부터 Payment Gateway에 보내진다.
(11) 인증 응답: 인증 응답은 Payment Gateway로부터 MPI에게 보내진다.

3-D Secure에서의 객체별 역할과 책임은 다음과 같다.

구분	역할과 책임
상점	- 상점은 MPI를 적용하거나, IPSP(Internet Payment Service Provider)로부터 서비스를 이용(e.g. WorldPay, Bibit)
매입사	- 상점를 등록
발행사	- ACS를 적용하고, 인증 메카니즘을 설정
카드소유자	- 카드소유자는 특별한 S/W나 장치를 사용할 필요가 없으며, 인증 메카니즘 적용에 대한 정의는 전적으로 발행사에게 의존
상호운영영역(VISA)	- Directory Server (유효 카드번호 체크) - 카드 스킴(e.g., VISA)가 승인한 CA (SSL 인증서 보증) - Authentication History Server (인증 결과 저장)

다음 표는 3-D Secure의 장점과 단점에 대한 비교표를 나타낸 것이다.

구분	내용
장점	- 카드소유자 인증을 위한 간단한 메카니즘 - 부가적인 S/W를 요구하지 않음 - 인터넷 접속이 가능한 장치를 이용한 사용자의 휴대성 제공 - 발행사가 카드소유자를 등록 - 논쟁 해결을 위한 Authentication History 존재 - 3D-SET 보다 간소함
단점	- ISP로부터 서비스를 받을 수 있는 MPI를 요구 - 지불정보(e.g. 카드 번호, 유효기간)가 상점 Server에 노출됨 - 적용 시점에서 Directory Server와 History 서비스를 위해 공개된 수수료 내역 결여 - 거래에 관련된 Directory Server의 트래픽 증가

3. 전자지불시스템 비교 분석

다음의 표는 여러 신용카드 기반 전자지불 시스템을 구성하는 각 개체별로 안전성(카드소유자의 인증), 채무에 대한 책임, 복잡도 측면에서 갖는 특성들을 요약한 것이다.

		SSL 기반	3D-SET	3-D Secure
카드소유자	인증	없음	있음	있음
	복잡도	매우 간단함	plug-in을 설치해야 함	만약 칩 카드가 사용되지 않는다면 추가적인 S/W 필요 없음
발행사	복잡도	부가적으로 변경할 필요가 없음	상당한 변경이 요구됨	상당한 변경이 요구됨
	채무	카드소지자가 부인하는 경우 환불이 있음. Intra-European 지불의 경우는 전적으로 책임이 있음	인증에 대한 카드소지자의 부인은 없음	인증에 대한 카드소지자의 부인은 없음
승인사	채무	지불 거부 (chargeback) 없음	지불 거부 (chargeback) 없음	지불 거부 (chargeback) 없음
상점	채무	카드소유자가 부인을 하는 경우 돈을 받지 못함	발행사가 지불을 보증함	발행사가 지불을 보증함
	복잡도	쉽게 변경 가능함	상당한 변경이 요구됨.	상당한 변경이 요구됨
	PAN, date	반드시 보호되어야 함	상점에게는 보이지 않음	반드시 보호되어야 함

4. 결론

본 논문에서는 SSL 기반, SET, 3D-SET, 3-D Secure의 개요, 객체별 역할과 책임, 장점/단점 등을 비교 분석하였다. 살펴본 바와 같이 과거에는 신용카드를 이용한 전자거래에서 사용되는 안전한 전자지불 시스템으로 SSL에 기반한 방식과 SET이 가장 대표적인 방식이었다. 그러나, 시장의 폭넓은 지지를 받고 있는 SSL 기반 방식은, 카드소유자 본인 확인 기능이 없는 단점이 있으며, 비자와 마스터카드가 개발한 SET은 상점에게 개인 정보가 노출되지 않는 장점은 있지만 기술적으로 복잡해 시장의 호응을 받지 못한 채 외면당해 왔다. 이러한 상황에서 안전한 인터넷 상의 안전한 전자지불을 위한 시스템이 요구되고, 이에 부응하기 위해 최근에 비자와 마스터카드가 3D-SET, 3-D Secure가 개발하였다.

3D-SET, 3-D Secure는 여러 부분에서 기술적인 차이를 보이고 있지만 모두 기존 신용카드 기반 전자지불이 제공해주지 못했던 카드소유자 인증 부분을 보완한 안전한 시스템이라는 공통점을 가지고 있다. 그러나, 과거에 발표되었던 SET이 여러 가지 우수함에도 불구하고 사용상의 불편함으로 시장의 호응을 얻지 못하고 사장된 것을 상기할 때 ID/패스워드의 등록 및 입력이라는 또 하나의 귀찮은 절차를 마련하는 것과 하나의 통합된 시스템이 아닌 다른 시스템의 적용이 과연 시장의 얼마만큼 호응을 받을 지는 좀 더 지켜보아야 할 것이다. 특히, 3-D Secure의 경우는 VISA사가 현재 시장의 호응을 받을 수 있도록 꾸준히 업그레이드 하고 있다.

따라서, 향후 개발되는 신용카드 기반 전자지불시스템은 안전성 측면에서는 카드 인증 뿐 만 아니라, 카드소유자 인증과정이 반드시 포함되어야 하고, 효율적인 측면에서도 간결하고, 발생되는 문제에 대한 책임소재를 명확히 할 수 있도록 시스템을 구성해야 할 것이다.

[참고문헌]

[1] European Committee For Banking Standards, "Secure Card Payments On The Internet", Version 1.0, November 2002. available at http://www.ecbs.org/

[2] European Committee For Banking Standards, "Secure Card Payments On The Addendum", Version 1.0, March 2003. available at http://www.ecbs.org/

[3] European committee for banking standards, "Guidelines On Algorithms Usage And Key Management", Version 2.0, September 2001. available at http://www.ecbs.org/

[4] GPayments-Authentication and Payment Solutions, "Visa 3-D Secure vs. MasterCard SPA", March 2002. available at http://www.gpayments.com/

[5] MasterCard, http://www.mastercard.com

[6] VISA, http://www.visa.com/

[7] ECBS, http://www.ecbs.org/

[8] GPayments, http://www.gpayments.com/