Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.563

SSL과 패스워드 기반의 신용카드 간편결제 프로토콜*

김 선 범,† 김 민 규, 박 종 환‡
상명대학교

Simple Credit Card Payment Protocols Based on SSL and Passwords*

Seon Beom Kim,† Min Gyu Kim, Jong Hwan Park‡
Sangmyung University

요 약

현재 국내에서는 다양한 신용카드 간편결제 프로토콜이 제시되고 있다. 제시되는 프로토콜의 특징은 사용자 인증을 위해 공인인증서 대신 패스워드를 사용하고, ActiveX를 통해 별도의 보안모듈을 설치할 필요가 없다는 것이다. 본 논문에서는 표준화된 보안 프로토콜인 SSL(Secure Socket Layer)과 패스워드 인증을 이용하여 두 개의 새로운 간편결제 프로토콜을 제안한다. 첫 번째는 온라인 쇼핑몰과 PG(Payment Gateway)가 다른 경우로써 국외의 페이팔(PayPal)을 이용한 간편결제와 유사하고, 두 번째는 온라인 쇼핑몰과 PG가 같은 경우로써 국외의 아마존(Amazon)에서 제공하는 결제방식과 유사하다. 제안되는 두 개의 프로토콜 모두 온라인 쇼핑 시, 쇼핑과정과는 독립된 별도의 사전등록절차를 요구하지 않고 쇼핑과정에서 자연스럽게 등록 및 결제를 처리할 수 있다. 또한 로그인 패스워드와는 다른 결제 패스워드를 입력하도록 하여 안전성을 향상시켰다. 본 논문에서 제시한 프로토콜은 현재 다양한 업체에서 제시하는 간편결제 프로토콜을 보다 더 정확하게 이해하고, 그 안전성을 분석하는데 도움이 될 것이다.

ABSTRACT

Recently, a plenty of credit card payment protocols have been proposed in Korea. Several features of proposed protocols include: using passwords for user authentication in stead of official certificate for authenticity, and no need to download additional security module via ActiveX into user's devices. In this paper, we suggest two new credit card payment protocols that use both SSL(Security Socket Layer) as a standardized secure transaction protocol and password authentication to perform online shopping and payment. The first one is for the case where online shopping mall is different from PG(Payment Gateway) and can be compared to PayPal-based payment methods, and the second one is for the case where online shopping mall is the same as PG and thus can be compared to Amazon-like methods. Two proposed protocols do not require users to perform any pre-registration process which is separate from an underlying shopping process, instead users can perform both shopping and payment into a single process in a convenient way. Also, users are asked to input a distinct payment password, which increases the level of security in the payment protocols. We believe that two proposed protocols can help readers to better understand the recent payment protocols that are suggested by various vendors, and to analyze the security of their payment protocols.

Keywords: Credit Card Payment Protocol, Password Authentication, Payment Gateway, SSL(Secure Socket Layer)

Received(12. 28. 2015), Modified(05. 17. 2016), Accepted(05. 17. 2016)
* 본 연구는 2015년도 상명대학교 교내연구비를 지원받아 수행하였음.

† 주저자, kymj1@naver.com
‡ 교신저자, jhpark@smu.ac.kr(Corresponding author)

I. 서 론

최근 국내에서는 온라인 쇼핑몰 시장의 일부 규제가 폐지되면서 신용카드 기반의 다양한 간편결제 프로토콜이 새롭게 제시되고 있다. 2014년 5월 공인인증서 의무사용 규제가 폐지되었고, 금융위원회와 미래창조과학부는 간편결제 방식 허용, 결제한도 금액 폐지, PG(Payment Gateway: 결제대행사)의 카드정보 허용 등 규제완화조치를 허용하였다. 이로 인해 신용카드 기반의 간편결제 시장이 성장하기 시작하면서, 2015년 말까지 제안된 약 16개가 넘는 신용카드 기반 간편결제 기법이 비교 분석되었다[1, 2, 3, 4 ,5 ,6 ,7 ,8]. 그 결과 현재 간편결제 기법에 대한 인지율이 97.9%이고, 이용 경험은 72.1%로 매우 높았으며 향후에는 더욱 더 많이 사용될 것으로 전망된다[9, 10]. 새로운 간편결제 프로토콜의 특징은 크게 두 가지로 요약할 수 있는데, 첫째, 공인인증서를 이용한 사용자 인증을 포기하고 전통적인 ID/PW 기반의 인증을 사용하는 것과, 둘째, SSL(Secure Socket Layer)과 같은 표준화된 방식으로 보안채널을 형성하고, 그 위에서 ID/PW로 사용자를 인증함으로써 ActiveX와 같은 별도의 보안모듈을 설치할 필요가 없다는 것이다[11].

이러한 장점에도 불구하고, 일부 간편결제 기법은 모바일 환경에 특화된 서비스를 제시하기 위해 모바일 어플리케이션을 설치해야 하거나, 온라인 쇼핑과정과는 별도로 사전에 사용자의 카드정보를 등록해야 하는 불편함도 존재한다. 별도의 어플리케이션을 사용자의 기기에 설치하는 것은 결국 ActiveX와 유사한 형태로 보안 모듈을 설치하는 것과 비슷하므로, 어플리케이션에 업데이트가 발생할 때마다 새로운 패치 또는 백신 프로그램을 추가적으로 설치해야 한다. 또한 하나의 쇼핑몰에서 지원하는 간편결제 어플리케이션이 다른 쇼핑몰에서 지원되지 않는다면, 결국 결제할 때마다 새로운 간편결제 어플리케이션을 설치해야 하는 문제가 발생한다. 이것은 표준화된 방식으로 구성이 가능한 간편결제 프로토콜의 장점을 무색하게 한다. 그리고 쇼핑과정과는 별도로 신용카드 정보의 사전등록(pre-registration)을 거쳐야 하는 것은, 쇼핑과정을 잠시 중단하고 새로운 사이트에 접속해야 하는 불편함을 초래한다. 더욱 사용자를 불편하게 하는 것은, 이러한 사전등록이 끝난 후 쇼핑과정을 처음부터 다시 시작해야 하는 경우이다.

본 논문에서는 새로운 신용카드 간편결제 프로토콜을 제시한다. 제안하는 프로토콜은 (1) ActiveX 또는 별도의 어플리케이션을 설치할 필요가 없고, (2) 공인인증서를 사용하지 않으며, (3) 쇼핑과정과 다른 별도의 사전등록절차가 아닌, 쇼핑과정의 일부로 (필요 시) 신용카드 등록절차가 이루어지며, (4) SSL과 패스워드만으로 간편결제를 처리할 수 있다. 따라서 제안하는 프로토콜은 표준화된 방식으로 설계가 가능하므로 Windows, Linux, iOS, Android 등의 운영체제, IE(Internet Explorer), Chrome 등의 웹브라우저, 그리고 PC나 노트북, 모바일 기기 등에서도 별다른 제약 없이 동작할 수 있다. 구체적으로 두 개의 프로토콜을 제시하는데, 첫 번째는 온라인 쇼핑몰과 PG가 다른 경우이고, 두 번째는 온라인 쇼핑몰과 PG가 같은 경우이다. 국외 사례와 비교하면, 첫 번째 프로토콜은 페이팔(PayPal)을 PG로 이용한 간편결제와 비슷하고[12], 두 번째 프로토콜은 아마존(Amazon)이 쇼핑몰과 PG를 겸하는 간편결제와 비슷하다[13]. V장에서 제안하는 프로토콜과 국외 간편결제 기법들과의 차이점이 제시될 것이다. 제안하는 두 개의 프로토콜은 현재 다양한 업체에서 제공되는 신용카드 간편결제 프로토콜을 더 정확하게 이해하고 그 안전성을 분석하는데도 도움이 될 것이다.

II. 간편 결제 프로토콜의 사전 지식

2.1 프로토콜 구성 객체

신용카드 간편결제 프로토콜은 사용자(user), 쇼핑몰(shopping mall), PG(payment gateway), 신용카드사(credit card company)로 구성된다. 각 주체별 역할은 다음과 같다.

- **사용자**: 온라인 쇼핑몰을 이용하여 물품을 구매하는 자
- **(온라인) 쇼핑몰**: 물품을 판매할 수 있는 쇼핑사이트를 개설한 웹서비스 제공자
- **신용카드사**: 사용자에게 신용카드를 발급해주고 사용자의 신용도에 따라 지불결제를 해주는 회사
- **PG**: 사용자와 쇼핑몰 간에 물품구매가 발생하면 그에 대응하는 카드결제정보를 신용카드사에 제공하고 결제업무를 처리하는 업체

2.2 객체별 안전한 통신에 대한 가정

기본적으로 사용자와 각 주체별 통신은 SSL을 이용한다고 가정하자. 구체적으로 다음과 같다.

- **사용자 ↔ 신용카드사:** 사용자는 신용카드사로부터 신용카드를 발급받고, 이를 (물리적으로) 수령한다. 이 경우 간편결제 프로토콜에서는 별도의 안전한 통신채널을 가정하지 않는다.
- **사용자 ↔ 쇼핑몰:** 쇼핑몰이 제공하는 웹사이트와 사용자의 웹브라우저 간에 SSL 통신이 이루어진다.
- **사용자 ↔ PG:** 쇼핑몰에서 결제정보가 PG로 전송되면 사용자의 웹브라우저와 PG 간에 SSL 통신이 이루어진다.

이외에 쇼핑몰과 PG 또는 PG와 신용카드사 간의 통신은 안전한 전용망(예를 들어 X.25 등) 또는 가상사설망(예를 들어 IPsec 등)을 이용하여 통신이 보호된다고 가정하자. 이러한 전용망 관련 보안 프로토콜은 본 논문의 범위를 벗어나므로 더 이상 논의하지 않는다.

2.3 사용자 인증에 대한 가정

결국 사용자 측면에서는 물품구매를 위해 쇼핑몰, PG과 각각 SSL 통신을 하게 된다. 여기서 언급하는 SSL 통신은 서버(여기서는 쇼핑몰, PG가 됨)가 보내주는 인증서(Certificate)를 이용하여 서버를 인증하고 키 교환을 통해 안전한 세션을 생성하는 것을 다룬다. 즉, 사용자는 인증을 위해 인증서를 소유하거나, OTP(one-time password)를 사전에 소유할 필요가 없다. 이 경우 사용자 인증을 위해 전통적인 ID/PW를 이용한다. 즉 SSL을 이용하여 서버 인증, 키 교환이 이루어지면, 그 안전한 채널 위에서 **사용자의 ID/PW로 사용자를 인증**하게 된다. 따라서 사용자 인증을 위해 별도의 ActiveX 또는 exe 파일 설치 등의 과정이 전혀 필요 없다. 단, 사용자가 입력하는 PW는 입력 단계에서 안전하게 보호된다고 가정하자.

III. PG와 쇼핑몰이 다른 경우 프로토콜

PG와 쇼핑몰이 서로 다는 주체로 분리되어 있는 경우이다. 이 경우 쇼핑몰 사이트에는 사용자들이 사용하는 신용카드로 결제할 수 있는 간편결제 프로토콜이 지원되어야 한다. 이러한 가정 하에서 간편결제 프로토콜을 구성한다. 프로토콜의 이해를 돕기 위해 사용자가 볼 수 있는 화면을 이용하여 설명한다.

3.1 프로토콜 설명

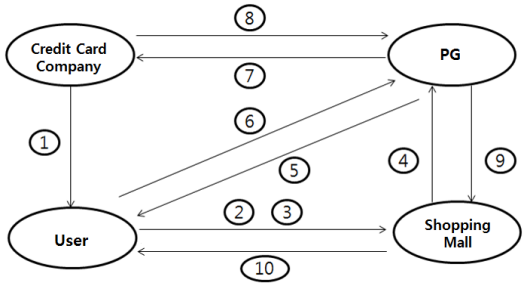

Fig. 1. Our payment protocol 1

1. 사용자는 신용카드사로부터 카드를 발급받는다.

2. 사용자는 물품을 구매하기 위해서 쇼핑몰 사이트에 접속한다. 이 경우 (쇼핑몰이 보내오는 인증서를 이용하여) SSL 통신을 수행함으로서 사용자는 쇼핑몰을 인증하고 안전한 채널을 생성한다. 그 SSL 통신 위에서 ID/PW로 사용자는 쇼핑몰에 자신을 인증한다. (즉 ID/PW로 로그인을 한다.) 이러한 로그인은 물품을 먼저 선택한 후 이루어질 수도 있다.

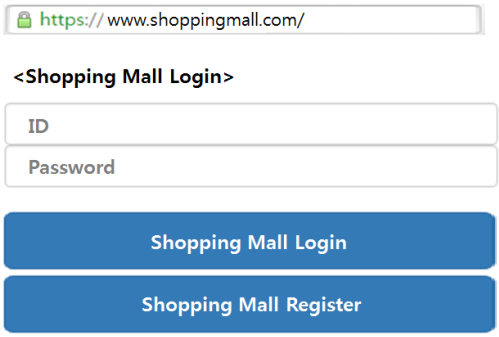

Fig. 2. Shopping Mall login

3. 사용자는 쇼핑몰에서 구매하고자 하는 물품을 선택한다. 그 다음 (로그인이 되어 있다는 가정 하에) 구매물품을 선택하고 '결제하기'를 클릭한다.

Fig. 3. Selection of goods

4. 쇼핑몰은 PG에 물품정보를 넘겨주고 결제 대행 서비스를 요청한다. 단, 필요할 경우 (현행 법률이 허용하는 범위 내에서) 사용자 정보도 함께 PG에 넘겨줄 수 있다.

5. PG는 쇼핑몰이 보내 온 정보를 바탕으로 사용자에게 결제에 필요한 정보를 요청하는 사용자 인증 화면을 보여준다. 아래 그림은 pgcompany라는 PG가 보내 온 인증서를 통해 사용자에게 PG를 인증하고, 안전한 채널을 형성하는 SSL 통신을 보여준다.[1)]

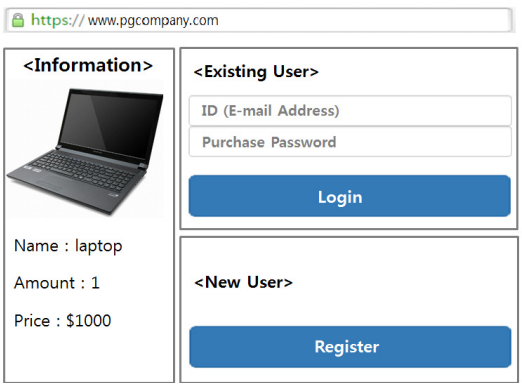

Fig. 4. Login for payment

6. 사용자 인증은 크게 두 가지 방법으로 수행된다. (1) **이전에 결제한 경우** - 이미 간편결제 서비스에 등록을 한 사용자는 등록 시 사용한 ID(e-mail 주소)와 '**결제PW**'를 입력하여 PG에 자신을 인증한다. 여기서 ID는 사용자의 e-mail 주소를 입력함으로서 아마존(Amazon)이나 페이팔(PayPal)처럼 국외 사용자들도 쉽게 사용할 수 있다. 또한 결제PW는 해당 신용카드로 결제 시 사용되는 PW로 쇼핑몰 사이트 가입 시 입력하는 PW와는 다른 것임을 상기하자. (2) **처음 결제하는 경우** - 사용자가 소유하는 신용카드 관련 정보를 입력하고, 간편결제 서비스에 등록한다. 여기서 ID는 사용자의 e-mail 주소를 이용하고, '결제PW'는 해당 신용카드 결제 시 사용하는 새로운 PW를 말한다. 사용자가 신용카드 소유자인지를 검증하기 위해 신용카드 수령 시 설정한 패스워드 네 자리 숫자 중 앞 두 자리만 입력하도록 한다. 이 PW는 사용자를 신용카드사에 인증하는 용도로만 사용하고, 이하의 프로토콜에서는 더 이상 사용되지 않는다. 요구되는 정보의 입력이 완료되면, 사용자는 다시 사용자 인증 화면으로 가서 ID/PW를 입력한다.

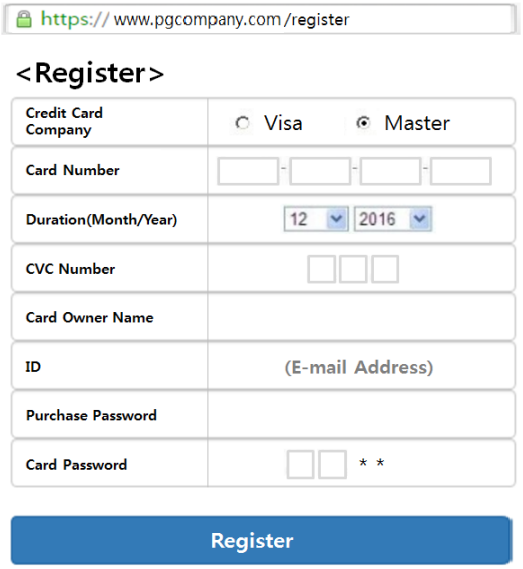

Fig. 5. New Registration

7. PG가 수행하는 방법은 사용자 인증방법에 따라 약간의 차이가 있다. (1) **이전에 결제한 경우** - 사용자가 보내온 ID/PW를 통해 사용자 인증을 수행한다. 사용자 인증이 정상적으로 이루어지면 PG는 사용자의 결제정보(PG의 DB에 포함된

1) 사용자가 여러 개의 신용카드를 등록한 경우, 해당 거래에서 어떠한 신용카드로 결제할 것인지에 대한 정보를 PG는 사용자에게 제공하여야 한다. 본 논문에서는 하나의 신용카드를 사용하는 경우만 고려한다.

사용자의 카드정보를 포함)를 신용카드사에게 전송하여 결제승인을 요청한다. (2) **처음 결제하는 경우** - PG는 사용자가 보내온 등록정보를 자신의 DB에 저장한다. 그 다음 (사용자 인증과정으로 입력된) ID/PW를 이용하여 사용자 인증을 수행한 후, 사용자의 결제정보를 신용카드사에게 전송하여 결제승인을 요청한다.

8. 카드사는 PG가 보내온 정보를 바탕으로 신용카드 소유자(즉 사용자)가 해당 결제금액을 지불할 수 있는지를 확인 후 결제승인정보를 PG에 전송한다.

9. PG는 신용카드사로부터 받은 결제승인정보를 다시 쇼핑몰에게 전송한다.

10. 쇼핑몰은 PG에게 받은 결제승인정보를 바탕으로 사용자에게 결제완료(결제승인 된 경우) 정보를 보여준다.

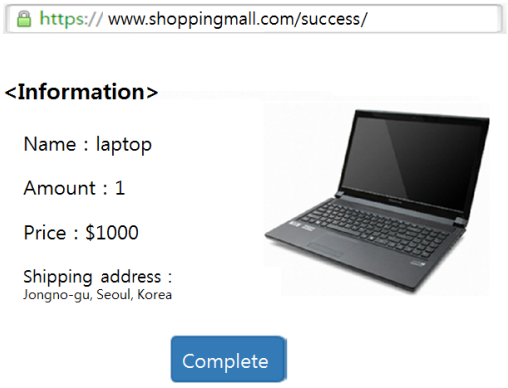

Fig. 6. Payment completion

3.2 프로토콜의 장점

위에서 설명한 신용카드 기반 간편결제 프로토콜의 장점으로는 (1) ID/PW를 이용한 간단한 사용자 인증(즉 사용자 인증서(certificate)가 필요 없는 것), (2) ActiveX가 필요 없는 것, (3) 결제절차와 독립적인 사전등록(pre-registration) 절차가 필요 없는 것, (4) 등록 후 결제 시에는 더 이상 카드번호가 노출되지 않는다는 것이다.

사용자 측면에서 물품구매를 위해 필요한 것은 두 개의 ID/PW 뿐이다. 즉, 쇼핑몰 로그인 시 필요한 ID/PW와 PG를 통한 결제 시 필요한 ID/결제PW이다. 사용자 인증을 위해 인증서(certificate)나 OTP 등 별도의 인증수단이 필요 없다. 특히 사용자 인증서를 사용하지 않으므로 (인증서에 있는 서명검증키(공개키)에 대응하는) 서명키를 저장하기 위해 별도의 NPKI 폴더와 같은 저장 공간을 마련할 필요가 없다. 따라서 이러한 서명키 저장문제를 해결하기 위한 별도의 클라이언트 모듈이나 ActiveX 등도 필요하지 않게 된다. 또한 SSL 통신을 이용하는데, 대부분의 웹서비스를 이용하는 프로토콜 주체들은 기본적으로 SSL 통신을 지원하는 프로그램을 설치하고 있다. 따라서 사용자 측면에서 쇼핑몰이나 PG와 안전한 통신 채널을 형성하기 위해 별도의 보안 클라이언트 모듈이나 ActiveX를 설치하지 않아도 된다. 마지막으로 사용자 측면에서 결제절차를 수행하는 도중, 이 절차와는 독립적으로 새로운 사전등록절차를 밟을 필요가 없다. 대부분의 사용자는 결제절차에서 벗어나 새로운 등록절차를 거친 후 원래의 결제절차로 오는 것을 매우 불편하게 여기므로 사용자 편의성 측면에서 이는 중요한 장점이 된다.

사용자가 처음 결제하는 경우, PG에게 신규등록정보를 전송하는 ⑥번의 과정을 수행하게 된다. 여기서 다양한 카드 정보 이외에 카드 비밀번호 중 일부를 요구하는 것은, 원래의 카드 소유자가 아닌 자가 결제를 시도하는 것을 막기 위해 필요하다. 사용자가 입력하는 (여러 카드정보 포함해서) 카드 비밀번호는 PG가 이 정보를 다시 신용카드사에게 보내서 실제 사용자가 카드 소유자인지를 인증하는 단계를 거친다. 즉 카드 비밀번호를 이용하여 사용자-PG-신용카드사로 구성되는 삼자간 인증 프로토콜을 거치게 되는 것이다. 여기서 생기는 의문점은 PG에게 사용자 카드 비밀번호 중 일부를 노출시키는 것이 과연 안전한가라는 것이다. 즉 PG에게 어느 정도의 신뢰를 주어야 하느냐의 문제가 생긴다. 본 논문에서는 PG에 대한 신뢰도가 높다고 가정한 경우이다. 만약 PG에 대한 신뢰도가 낮다면, 사용자 카드 비밀번호는 (사용자가) 전혀 입력하지 않는 것으로 바뀔 것이다. 이 경우 타인의 카드를 도용하는 자는 쉽게 카드상의 정보만으로 결제과정을 진행할 수 있는 문제가 발생할 수 있다. 이를 완화하기 위해서 사용자는 자신이 결제한 내역을 신용카드사로부터 직접 (e-mail 등을 이용하여) 통보받고, 일정 기간 동안은 해당 결제를 취소할 수 있는 권리가 주어지는 것이 바람직할 것이다. 또한 신용카드사나 PG는 타인의 도용으

로 인한 사고를 사전에 방지하기 위해 실시간 이상거래탐지시스템(FDS: Fraud Detection System)을 도입하거나, 사회적 보험에 가입하여 사후적으로 사용자를 구제하는 것도 필요할 것이다. 이러한 사전/사후 해결책들은 전자결제에서의 인증방법과 관련된 법제도도 함께 고려되어야 하는 것으로서 본 논문의 연구범위를 벗어나므로 생략한다. 단 여기서는 PG에 대한 신뢰도가 높다고 가정한 경우만 다룬다.

IV. PG와 쇼핑몰이 같은 경우 프로토콜

앞서 살펴본 프로토콜의 경우 PG와 쇼핑몰이 다른 경우였으나, 예를 들어 아마존(Amazon)처럼 일부 쇼핑몰은 자체 PG를 운영함으로써 PG 업무를 쇼핑몰 업무와 함께 하는 경우도 있다. 이 경우 PG와 쇼핑몰이 같다고 가정하고 프로토콜을 구성한다.

4.1 프로토콜 설명

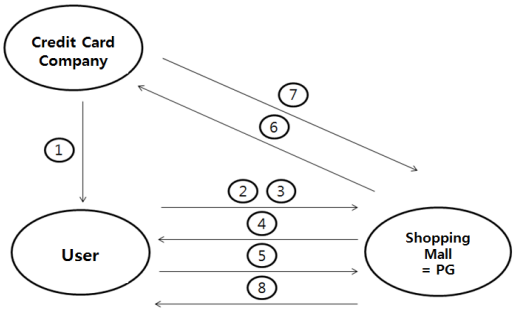

Fig. 7. Our payment protocol 2

1. 사용자는 신용카드사로부터 카드를 발급받는다.

2. 사용자는 물품을 구매하기 위해서 쇼핑몰 사이트에 접속한다. 이 경우 (쇼핑몰이 보내오는 인증서를 이용하여) SSL 통신을 수행함으로서 쇼핑몰을 인증하고 안전한 채널을 생성한다. 그 SSL 통신 위에서 ID/PW로 사용자는 쇼핑몰에 자신을 인증한다. (즉 ID/PW로 로그인을 한다.)

3. 사용자는 쇼핑몰에서 구매하고자 하는 물품을 선택한다. 그 다음 (로그인이 되어 있다는 가정 하에) 구매물품을 선택하고 '결제하기'를 클릭한다.

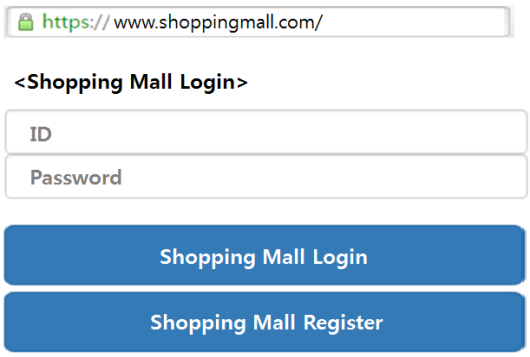

Fig. 8. Login to Shopping Mall

Fig. 9. Selection of goods

4. 쇼핑몰은 사용자에게 결제에 필요한 정보를 요청하는 사용자 인증 화면을 보여준다. 여전히 쇼핑몰이 보내온 인증서를 이용하여 SSL 통신을 맺고 그 위에서 사용자에게 인증을 요청하게 된다.

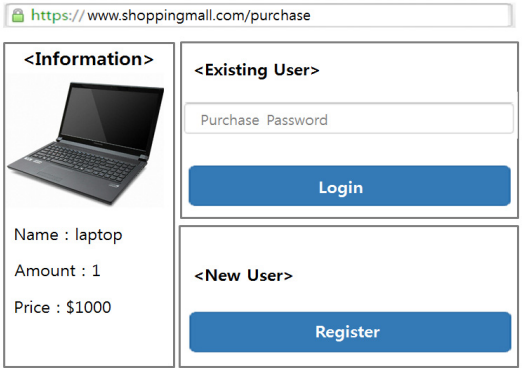

Fig. 10. Login for payment

5. 사용자 인증은 크게 두 가지 방법으로 수행된다. (1) **이전에 결제한 경우** - 이미 간편결제 서비스에 등록을 한 사용자는 '**결제PW**'만 입력하여 쇼핑몰(=PG)에게 자신을 인증한다. 여기서도 결제PW는 해당 신용카드로 결제 시 사용되는 PW로 쇼핑몰 사이트 로그인 시 입력한 PW와는 다른 것임을 상기하자.[2] (2) **처음 결제하는 경우** - 사용자가 소유하는 신용카드 관련 정보를 입력하고, 간편결제 서비스에 등록한다. 신용카드 상에 노출된 정보뿐만 아니라, 카드 비밀번호의 일부도 입력한다.[3] III장의 프로토콜과 다른 점은 사용자 ID를 요구할 필요가 없다는 것이다. 이는 이미 쇼핑몰(=PG) 로그인 시 사용자 ID가 특정되었기 때문에 추가적인 ID 요청은 불필요하기 때문이다. 요구되는 정보의 입력이 완료되면, 사용자는 다시 사용자 인증 화면으로 가서 결제PW를 입력한다.

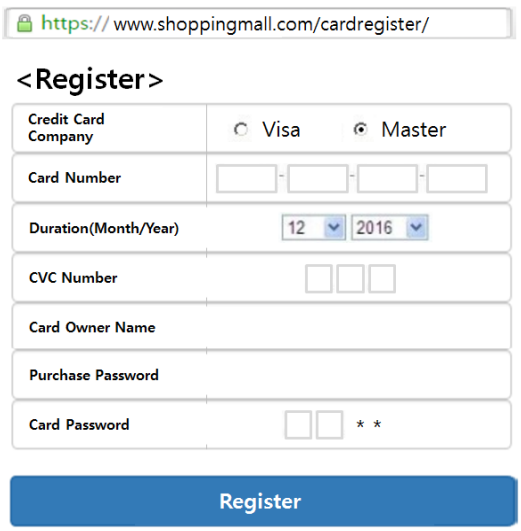

Fig. 11. New Registration

6. III장의 프로토콜과 마찬가지로 쇼핑몰은 사용자 인증방법에 따라 다르게 수행한다. (1) **이전에 결제한 경우** - 사용자가 보내온 결제PW를 통해 사용자 인증을 수행한다. 사용자 인증이 정상적으로 이루어지면 쇼핑몰(=PG)는 사용자의 결제정보(쇼핑몰(=PG)의 DB에 포함된 사용자의 카드정보를 포함)를 신용카드사에게 전송하여 결제승인을 요청한다. (2) **처음 결제하는 경우** - 쇼핑몰은 사용자가 보내온 등록정보를 자신의 DB에 저장한다. 그 다음 (사용자 인증과정으로 입력된) 결제PW를 이용하여 사용자 인증을 수행한 후, 사용자의 결제정보를 신용카드사에게 전송하여 결제승인을 요청한다.

7. 신용카드사는 쇼핑몰(=PG)이 보내온 정보를 바탕으로 신용카드 소유자(즉 사용자)가 해당 결제금액을 지불할 수 있는지를 확인 후 결제승인정보를 쇼핑몰에 전송한다.

8. 쇼핑몰은 신용카드사에게 받은 결제승인정보를 바탕으로 사용자에게 결제완료(결제승인 된 경우) 정보를 보여준다.

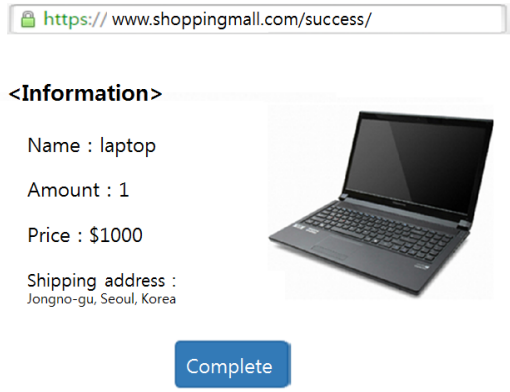

Fig. 12. Payment completion

4.2 프로토콜의 장점

위에서 설명한 신용카드 기반 간편결제 프로토콜의 장점 역시 III장과 마찬가지로 (1) ID/PW를 이용한 사용자 인증(즉 사용자 인증서(certificate)가 필요 없는 것), (2) ActiveX가 필요 없는 것, (3) 결제절차와 독립적인 사전등록(pre-registration) 절차가 필요 없는 것, (4) 등록 후 결제 시에는 더 이상 카드번호가 노출되지 않는다는 것이다.

또한 쇼핑몰과 PG가 같음으로서 생기는 장점은 III장의 프로토콜에 비해 (a) 전체적인 프로토콜 흐

2) 물론 사용자에 따라서는 쇼핑몰 로그인 PW와 결제 PW를 동일한 것으로 설정하는 경우도 있을 것이다.

3) 앞서 언급한대로, 본 논문에서는 PG의 신뢰도가 높다고 가정하는 경우이다. PG의 신뢰도가 낮다면 카드 비밀번호를 입력하지 않도록 수정될 것이다.

름(flow)이 줄어들어 전체적으로 통신비용이 줄게 되고, (b) 쇼핑몰에서 PG로 웹브라우저가 전환되는 것도 필요하지 않으며, (c) 사용자는 쇼핑몰과 SSL 통신을 한번만[4] 맺으면 되므로 SSL 통신을 맺는데 드는 비용을 줄이게 되고, (d) 사용자가 로그인 시 이미 쇼핑몰(=PG)은 사용자가 사용할 카드번호를 알게 되므로 결제 시 카드번호의 일부(예를 들어 마지막 네 자리 숫자)를 보여줌으로써 현재 어떤 카드로 결제중인지를 알려 줄 수 있다.

사용자 측면에서는 물품구매를 위해 필요한 것으로 한 개의 ID와 두 개의 PW 뿐이다. 즉, 쇼핑몰 로그인 시 필요한 ID/PW와 결제 시 필요한 결제 PW이다. 그러므로 쇼핑몰에 로그인 후 사용자가 이전에 구매한 경력이 있다면, 새로운 구매 시에는 단순히 결제PW만 입력하면 결제가 완료된다. 또한 쇼핑몰 로그인 PW와 결제PW가 동일하게 설정했다면, 사용자는 하나의 PW만 기억함으로서 간편결제를 완료할 수 있게 된다. 그러나 이것은 사용자 편의성은 증대될 수 있으나, 안전성은 약화시킬 것이다.

여기서도 쇼핑몰(=PG)에 대한 신뢰도를 높게 가정하는 경우만을 고려한다. 만일 쇼핑몰에 대한 신뢰도가 우려스럽다면, 사용자는 해당 쇼핑몰과 거래하는데 주저할 것이다.

V. 페이팔 및 아마존과의 간편결제 비교

5.1 페이팔(PayPal)과의 비교

페이팔은 신용카드 간편결제 프로토콜에서 사용자와 쇼핑몰 간의 결제과정을 대행하는 PG이다. 따라서 페이팔을 이용하는 간편결제는 PG와 쇼핑몰이 다른 경우로 볼 수 있다. 실제 페이팔을 이용하려면, 사용자는 사전에 등록과정으로 자신의 신용카드 정보와 e-mail 주소, 결제PW를 페이팔에 등록해야 한다. 나중에 쇼핑몰에서 물품을 선택 후 결제단계에서 페이팔을 선택하면, 페이팔은 사용자에게 이메일 주소와 결제PW를 입력하도록 요청한다. 이러한 사용자 인증 정보가 정확히 입력되면 PG는 미리 등록된 사전 정보를 이용하여 신용카드 사용자를 인증하고 이후의 결제 프로세스를 진행한다.

전체적으로 본 논문에서 제시하는 방법과 유사하지만, 중요한 차이점은 사용자가 반드시 페이팔이라는 PG사에 접속하여 자신의 카드정보를 사전등록해야 된다는 것이다. 이러한 사전등록은 온라인 쇼핑과정과는 별도로 진행되어야 하므로, 만일 페이팔 사전등록을 하지 않은 사용자라면, 쇼핑몰에서 물품을 선택한 과정과는 별도로 페이팔 사전등록 과정을 독립적으로 수행한 후 다시 쇼핑몰에 접속해야 하는 불편함이 존재한다. 안전성 측면에서는 제안하는 기법이 페이팔에 비해 더 우수한데, 이는 타인의 카드를 획득한 자가 카드 도용을 시도하는 경우에 확실히 구분된다. 페이팔의 경우 사전등록 시 필요한 정보는 모두 카드로부터 알 수 있는 정보들로 구성되어 있어 타인의 카드로 쉽게 사전등록을 하고 결제를 완료할 수 있다. 그러나 제안된 기법에서는 카드정보 이외에 카드 비밀번호 두 자리를 추가적으로 요구하므로 타인의 카드 도용이 어려워진다. 물론 이 경우 카드 비밀번호 입력이 일정 횟수 이상 실패하면 실시간 이상거래탐지시스템(FDS)을 통해 이상거래로 식별할 것이다. Table 1에서는 본 논문에서 제시하는 간편결제 프로토콜 1(즉 쇼핑몰과 PG가 다른 경우)과 페이팔을 PG로 이용하는 프로토콜을 비교한다.

Table 1. Comparison between our protocol 1 and PayPal-based protocol

	Our protocol 1	PayPal-based
Active X	No	No
User certificate	No	No
Pre-registration (to PG)	No	Yes
User authentication	Log-in PW, Payment PW	Log-in PW, Payment PW
Secure channel	SSL	SSL
App download	No	No

5.2 아마존(Amazon)과의 비교

아마존은 온라인 쇼핑몰과 PG의 역할을 동시에 수행하는 업체이다. 따라서 사용자는 아마존에서 물품을 구매할 때, 사전등록이 되어 있지 않아도 자연스럽게 신용카드 정보를 등록하면서 결제과정을 진행할 수 있다. 그리고 최초의 신용카드 등록과정을 거쳐 결제가 완료되면, 해당 신용카드 정보는 아마존 서버에 저장되고 이후의 결제에서는 사용자 로그인과 동시에 해당 사용자의 신용카드 정보를 사용할 준비

4) III장의 프로토콜은 사용자가 쇼핑몰 및 PG와 각각 한번씩 SSL 통신을 맺는 것이 필요하다.

를 하게 된다. 따라서 (한번 결제한 이후 해당 카드가 여전히 유효하다면) 결제에 필요한 별도의 결제 PW를 요청하지 않으므로, 사용자는 단순히 아마존 로그인 시 입력한 로그인 PW만으로 결제과정을 완료할 수 있다. 더욱이 사용자 접속정보를 아마존에 전달하는 쿠키(cookies)를 사용할 경우, 사용자는 로그인 PW를 입력할 필요도 없이 아마존 사이트에 접속하는 것만으로 온라인 쇼핑과 결제를 할 수 있게 된다. 그러나 쿠키는 인증 프로토콜의 안전성에 문제를 야기할 수 있어 장려되지는 않는다.

본 논문에서 제시하는 간편결제 프로토콜 2(쇼핑몰과 PG가 같은 경우)와의 차이점은, 결제에 필요한 결제PW를 요청하는지 여부이다. 즉 제안하는 프로토콜에서는 로그인 PW와 다른 결제PW를 요청하지만, 아마존은 로그인 PW 하나만으로 로그인과 결제에 필요한 사용자 인증을 수행한다. 즉 제안하는 프로토콜 2에서는 결제 과정을 분리하여 신용카드와 연관된 사용자를 추가로 인증한다는 것이 중요한 차이점이다. 이로 인해 아마존 방식은 여러 장의 카드에 관계없이 하나의 로그인 PW만으로 간편결제가 이루어지나, 제안하는 방식은 카드별로 결제PW를 다르게 설정할 수 있다. 자연스럽게 편리성 측면에서는 아마존 방식이 우수하나, 안전성 측면에서는 제안하는 방식이 우수하다. Table 2에서는 본 논문에서 제시하는 간편결제 프로토콜 2(즉 쇼핑몰과 PG가 같은 경우)와 아마존 방식을 비교한다.

Table 2. Comparison between our protocol 2 and Amazon-like protocol

	Our protocol 2	Amazon-like
Active X	No	No
User certificate	No	No
Pre-registration (to PG)	No	No
User authentication	Log-in PW, Payment PW	Log-in PW
Secure channel	SSL	SSL
App download	No	No

VI. 결 론

공인인증서 의무사용 규제가 폐지됨에 따라, 현재 국내에서는 다양한 신용카드 간편결제 프로토콜이 제시되었다. 이러한 프로토콜은 ActiveX와 같은 보안 모듈을 사용자 기기에 설치할 필요가 없고, 사용자 인증을 위해 공인인증서 대신 패스워드를 이용하고 있다. 아직 소액결제 단계에서 주로 사용되고 있으나, 편리함을 장점으로 점차 사용빈도가 급격히 증가할 것으로 예상된다. 이러한 간편결제 프로토콜 구성은 온라인 쇼핑몰과 PG가 다른지 여부에 따라 전혀 다르게 프로토콜이 설계된다. 현재 시행되는 신용카드 간편결제 프로토콜들을 명확히 이해하고 그 안전성 분석을 용이하게 할 수 있도록, 본 논문에서는 두 개의 간편결제 프로토콜을 제안하였다. 첫 번째 프로토콜은 온라인 쇼핑몰과 PG가 다른 경우로써 국외의 페이팔(PayPal)을 PG로 이용하는 방식과 비교되고, 두 번째 프로토콜은 온라인 쇼핑몰과 PG가 같은 경우로써 국외의 아마존(Amazon) 방식과 비교될 수 있다. 새롭게 제안되는 두 개의 프로토콜 모두 로그인 패스워드와는 다른 결제 패스워드를 추가로 요구함으로써 안전성을 높였으며, 표준보안방식인 SSL을 이용함으로써 운영체제나 웹브라우저, 그리고 사용자 기기에 아무런 제약 없이 설계할 수 있다. 또한 모바일 환경에서도 별도의 결제 어플리케이션을 배포할 필요 없이 사용할 수 있다는 장점을 가진다.

References

[1] Yeong Ui Kim, Hyeon Sil Mun, Jae Kyeong Kim, "Analysis of competitive composition of mobile payment market," The Korea Society of Management Information Systems, pp.395-401, Nov. 2015.

[2] Jeong Gi Seog, "A study on Activation Measures of Local Mobile Easy-to-use Payment," Convergence security journal, 15(4), pp.79-88, Jun. 2015.

[3] Seung Hun Noh, Tae Gyeong Gwon, "A comparative study of easy payment services in the domestic mobile system environment," The Korea Society of Management Information Systems, pp.695-698, Nov. 2014.

[4] Hyeyoung Oh, "Referred Articles : A Study of Factors Affecting the Adoption Intention of Mobile Easy Payment Service," Journal of Financial Consumers, 5(1), pp.33-64, Aug. 2015.

[5] APPSTORY, Deok Su Choe, "Market of

moblie payment, the paradigm is chagned from today," http://monthly.appstory.co.kr/plan6500, Nov. 2014.
〔6〕 inews24, Eun Mi Jeong "The warring states period is comming to 'Market of easy payment'," http://navercast.naver.com/magazine_contents.nhn?rid=2033&contents_id=83298, Feb. 2015.
〔7〕 Cheol Yeong Kim, "Market of easy payment - 'Pay war' will be intensified during the second half and the market of easy payment be expanded," Hyundai Able Daily, Jul. 2015.
〔8〕 Han-na Chin, Seok-Cheon Park, Won-Tae Choi, "Analysis of Mobile Easy Payment Technology by the FinTech," Korean Society For Internet Information, pp.237-238, Oct. 2015.
〔9〕 Monthly App, "The actuality of utilization of mobile easy payment service," http://navercast.naver.com/magazine_contents.nhn?rid=2598&contents_id=91569, Jun. 2015.
〔10〕 APPSTORY, Seon Ung Choe, "The final round of the domestic easy payment services," http://monthly.appstory.co.kr/plan6913, Mar. 2015.
〔11〕 Seungchul Park, "A Comparative Analysis of NPKI and SSL/TLS for Secure Internet Transactions," Journal of Korea Institute of Information and Communication Engineering, 20(2), pp.289-298, Feb. 2016.
〔12〕 PayPal, http://www.paypal.com.
〔13〕 Amazon. http://www.amazon.com.

〈저자소개〉

김 선 범 (Seon Beom Kim) 학생회원
2016년 2월: 상명대학교 컴퓨터과학과 졸업
〈관심분야〉 인증 및 키 교환, 암호 프로토콜

김 민 규 (Min Gyu Kim) 학생회원
2016년 2월: 상명대학교 컴퓨터과학과 졸업
〈관심분야〉 인증 및 키 교환, 운영체제 보안

박 종 환 (Jong Hwan Park) 정회원
1999년 2월: 고려대학교 수학과 졸업
2004년 2월: 고려대학교 정보보호대학원 석사
2008년 8월: 고려대학교 정보보호대학원 박사
2013년 9월~현재: 상명대학교 컴퓨터과학과 조교수
〈관심분야〉 함수 암호, 브로드캐스트 암호, 암호 프로토콜