온라인 전자결제에서 금융정보 보호를 위한 Two-Session 을 이용한 결제시스템

예두희*, 김인환*, 송주석*
*연세대학교 컴퓨터과학과
e-mail : dhye@emerald.yonsei.ac.kr, inhwan@emerald.yonsei.ac.kr jssong@emerald.yonsei.ac.kr

Two-Session online payments system which protect financial information leakage in online electronic payments system.

Du-Hee Ye*, In-Hwan Kim*, Joo-Seok Song*
*Dept. of Computer Science, Yonsei University

요 약

온라인 전자 상거래 시장은 인터넷의 발전과 그 편의성으로 인하여 지속적으로 시장 규모가 커지고 있다. 비대면 결제방식인 온라인 전자결제 방식은 오프라인 결제 방식에 비해 높은 수준의 안전성이 요구된다. 결제정보가 노출된다면 공격자는 타인의 결제정보를 이용하여 불법적인 결제가 가능할 것이다. 현재 사용되고 있는 온라인 결제 시스템들은 결제정보를 안전하게 전송하기 위한 프로토콜을 구성하고 있지만 실제 해킹을 통한 결제정보 유출로 인해 최근 몇 년간 다수의 금융사고들이 일어나고 있다. 본 논문은 Two-Session 결제 방식을 이용해 국내 온라인 결제 시스템을 보완하여 향상된 보안성으로 결제정보를 전송하여 결제정보의 유출을 예방하고 기존 시스템 대비 높은 사용자 편리성을 가지는 시스템을 제안한다.

1. 서론

온라인 전자 상거래 시장의 활성화로 사용자들은 온라인을 통해서 보다 간편하게 상품을 구입할 수 있게 되었다. 그러나 온라인 전자거래의 경우 오프라인과는 다르게 비대면식 방식으로 결제가 진행되므로 해킹에 의한 결제정보 유출과 타인의 부정사용 방지를 위한 사용자 인증이 필수적이다.

현재 국내 온라인 전자결제의 대표적인 방법으로는 인터넷안전결제(ISP)와 안심클릭(VISA 3D-Secure)이 있다. ISP 결제의 경우 결제과정에서 카드번호를 매번 입력하지 않기 때문에 카드번호 유출로 인한 사고를 방지 할 수 있으나 추가적인 인증서를 발급받아 소유하고 있어야 한다는 단점이 있다. 하지만 결제 프로세스가 간단하고 End-to-End 암호화로 정보유출을 막을 수 있다.

안심클릭의 경우 결제 과정에서 매번 카드번호와 CVC 번호, 안심클릭 비밀번호를 입력해야 한다. 사용자는 매번 이러한 과정을 수행하므로 ISP 비밀번호만을 요구하는 ISP 결제 방식에 비해 사용자 편의성 측면에서 불편함을 가질 수 있다. 또한 이러한 일련의 절차는 공격자의 키로깅(Key-logging)에 의한 결제정보 탈취에 취약성을 가진다.

본 논문에서는 2-Session 을 이용한 결제시스템을 구성하여 기존 시스템의 보안적 취약점을 보완하고 사용자 편의성 측면에서 보다 간편한 방법으로 결제가 가능한 시스템을 제안하고자 한다.

2. 국내 온라인 결제 시스템과 취약점 분석

카드기반의 온라인 결제서비스 이용 시 결제정보 유출에 따른 위협은 꾸준히 제기 되어 왔다. 이에 각 온라인 결제 시스템들은 고유의 방법으로 결제 정보를 보호하고 사용자를 인증하는 시스템을 운영하고 있다. 그럼에도 불구하고 결제 정보 유출로 인한 금융사고는 지속적으로 발생하고 있다.

■ 인터넷 안전결제(Internet Secure Payment)

인터넷 안전결제(ISP)는 PKI 기반의 전자서명을 결제에 이용하는 시스템이다. 사용자는 ISP 인증서를 발급받아 암호화 되어있는 인증서를 이용해 결제에 이용한다. 사용자의 개인키로 서명한 인증서를 전송함으로써 사용자 인증과 결제정보 전송을 가능하게 한다. 인증서의 유효성을 발급기관에서 확인한 후 결제정보를 카드사에 전송함으로써 승인이 이루어진다. 사용자 측면에서 볼 때 사용자는 ISP 인증서를 소유하고 ISP 비밀번호 입력만으로 결제가 가능하다.[1][2][3]

기존의 Key-in 방식이나 안심클릭 시스템에서는 카드번호 등의 결제정보를 사용자에게 직접 입력 받아야 하지만 ISP 결제는 ISP 인증서 비밀번호만 입력하

면 결제가 진행된다. 그러나 인증서 기반의 시스템으로 인증서 관리 소홀로 인한 취약점이 있다.[5][6][7][8] 공격자가 인증서 탈취 후 인증서 비밀번호를 알아 낸다면 타인의 결제정보를 이용에 결제가 가능하다. 이러한 취약점은 실제로 2012 년 인증서의 유출로 인한 대규모 금융사고의 발생원인으로 알려졌다.

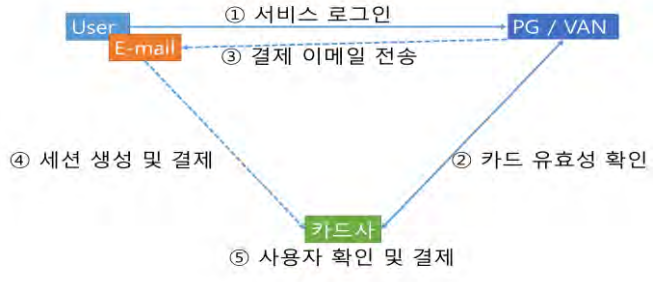
■ VISA 안심클릭(VISA 3D-Secure)

안심클릭 서비스는 VISA 의 3D-Secure 서비스를 변형한 서비스이다. 3D-Secure 서비스는 3-Domain 개념(발급사 영역, 매입사 영역, 상호운영 영역)에 기반하고 있으며 각 도메인의 권리와 의무를 명확하게 정의하는 모델이다. 서비스는 카드 승인단계와 지불인증 단계가 분리 되어 카드사가 고객을 직접 인증하는 방식을 취함으로써 타인에 의한 부정사용을 최소화하고자 하는 시스템이다. 사용자는 결제 시 카드번호와 CVC, 안심클릭 비밀번호를 입력하면 판매자의 플러그인이 카드사와 통신하여 승인인증 단계를 거치고 결제정보를 사용자 플러그인에서 카드사로 전송하여 결제 인증을 거치게 된다.[1][2][3][12]

안심클릭은 사용자가 결제 시 안심클릭 비밀번호와 함께 카드정보를 입력해야 한다. 매번 같은 과정을 반복해야 하므로 ISP 결제에 비해 낮은 사용자 편의성을 가진다. 또한 입력과정이 반복되므로 악성코드나 키로깅 프로그램에 의해 결제정보가 유출될 수 있다. SSL 로 카드정보를 판매자의 결제 모듈로 안전하게 전송하더라도 판매자 측의 해킹 피해로 결제 정보가 유출될 수 있다. 판매자의 결제모듈로 전송 받는 결제정보를 탈취 할 수 있기 때문이다. 가짜 웹사이트를 이용한 피싱이나 파밍 공격의 경우 사용자의 카드정보는 보다 더 쉽게 유출 가능하다. 안심클릭은 2010 년과 2012 년 결제정보 유출로 인한 부정사용으로 금융사고가 발생했다. [5][6][7][8][9]

3. Two-Session 을 이용한 온라인 결제시스템

앞서 Ⅱ절 에서 언급했듯이 국내에서 가장 많은 사용자를 보유하고 있는 시스템들은 보안 측면에서 취약점을 가지고 있고 실제 취약점을 이용한 결제정보 유출, 부정사용 등의 사고가 지속적으로 발생하고 있다 [9][10][11]. 또한 사용자 편의성 측면에서도 인증서를 보관하거나, 결제정보를 매번 입력해야 하는 등의 불편함을 가지고 있다.



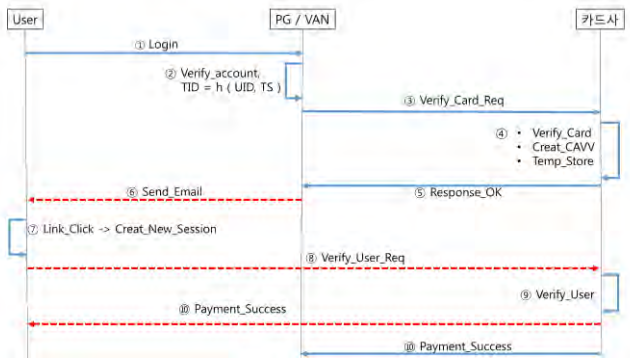
(그림 1) Two-Session 온라인 결제시스템 구조

본 논문에서는 사용자 인증 세션과 결제 승인 세션을 분리하여 거래 진행하는 온라인 결제 시스템을 제안한다. 시스템의 전체 구성은 (그림 1)과 같다.

사용자는 결제시스템을 사용하기 위해 서비스 가입 후 결제가 가능하다. 전자지급결제대행업체(Payment Gateway, 이하 PG) 데이터베이스에는 사용자정보(사용자 아이디, 이메일 주소)와 결제승인에 필요한 카드정보(카드번호, CVC 등)가 저장되어 있다. 결제는 사전에 PG 사에 저장된 정보로 진행되며 추가적인 인증서나 카드번호 입력 없이 회원가입 시 등록한 아이디와 비밀번호로 결제를 진행 한다.

(그림 1)과 같이 결제를 위해 사용자는 PG 사에 로그인 하게 된다. PG 사는 사용자가 회원가입 시 등록한 카드가 사용가능 한지 유효성을 확인 하기 위해 카드회사에 카드정보를 전송하고 응답을 받는다. 유효한 카드임을 확인 한 후 PG 사는 사용자가 서비스 가입시 등록한 이메일로 결제메일을 전송한다. 이메일 본문에는 결제 승인 과정을 진행하기 위한 새로운 링크를 전문에 포함하고 있다. 사용자가 링크를 클릭하게 되면 결제단계가 진행된다. 링크를 클릭하면 사용자의 IP 주소가 PG 사에 전송된다. 이 IP 주소는 사용자가 로그인시에 접속한 IP 주소와 일치함을 판단한다. PG 사는 사용자 일치 여부를 확인한 후 카드사와 통신하여 결제 승인을 받고 거래를 완료한다. 이 과정에서 일정시간 이내에 이메일에 첨부된 새로운 링크가 연결되지 않는다면 PG 사에서 거래를 자동으로 취소하게 된다.

■ 세부 데이터 전송 과정



(그림 2) Two-Session 을 이용한 세부데이터 전송

1) Login { UID || PW || IP_addr }

사용자는 주문정보를 입력하고 결제를 위해 PG 사의 결제시스템 로그인한다. 이때 사용자의 IP 주소도 함께 PG 사 로 전송된다.

2) Verify_account { UID || PW }
TID = h (UID, TS)

PG 사는 사용자의 계정정보를 확인하고 사용자 아이디(UID)와 타임스탬프(TS)를 해쉬함수를 이용해 거래 ID(TID)를 생성한다.

3) Verify_Card_Req { E_{Card_PK}(Pay_Info || Card_Info || IP_addr || TID) }

PG 사는 서비스 가입 시 저장한 사용자의 카드정보가 유효한지 확인하기 위해 카드사에 사용자의 카드

정보를 전송해야한다. 이때 2)에서 생성한 거래 ID 와 함께 결제에 사용될 카드정보와 사용자가 구매한 물건의 금액이 포함된 결제정보, 사용자가 접속한 IP 주소를 카드사의 공개키로 암호화 하여 전송한다.

4) Verify_Card{ $D_{Card\_PK}(E_{Card\_PK}($ *Pay_Info || Card_Info || IP_addr || TID)) }*

Creat_CAVV ( )

Temp_Store { TID || Card_Info || Pay_Info || IP_addr }

카드사는 전송 받은 메시지를 카드사의 개인키로 복호화 하여 카드정보가 결제가능한 유효카드인지 확인한다. 유효카드임을 확인 한후 결제가능한 카드임을 나타내는 CAVV 코드를 생성한다. 이후 거래 아이디와 카드정보, 결제정보, 사용자의 IP 주소를 임시 저장한다.

5) Response_OK { $E_{Card\_SK}($ *CAVV || TID) }*

카드사는 PG 사에 결제가 가능한 카드임을 알린다. 이때 카드정보는 4)에서 생성한 승인코드와 거래 ID 를 카드사의 대칭키로 암호화하여 전송한다.

6) Send_Email{ $E_{Card\_SK}($ *CAVV || TID) }*

PG 사는 서비스 가입시 등록한 사용자의 이메일로 결제를 진행할 메일을 전송한다. 메일전문에는 5)에서 카드사가 대칭키로 암호화하여 전송한 인증코드 CAVV 와 거래 ID 인 TID 를 첨부한 링크가 전달된다.

7) Link_Click -> Creat_New_Session ( )

사용자가 메일로 첨부된 링크를 클릭하면 결제를 위해 사용자와 카드사간 새로운 세션이 연결된다.

8) Verify_User_Req { $E_{Card\_SK}($ *TID ||* $CAVV)$ *||* $E_{Card\_PK}($ *IP_addr) }*

사용자 메일의 링크를 클릭하면 사용자와 카드사간 연결된 새로운 세션을 통해 첨부된 TID, CAVV 쌍과 현재 사용자가 연결된 IP 주소 정보를 사용자측에서 카드사로 전송한다. 이때 TID 와 CAVV 는 카드사가 대칭키로 암호화하여 메일에 첨부한 그대로 전송하고 IP 주소의경우 카드사의 공개키를 이용해 암호화하여 전송한다.

9) Verify_User { $D_{Card\_SK}($ $E_{Card\_SK}($ *TID || CAVV)) ||* $D_{Card\_PK}($ $E_{Card\_PK}($ *IP_addr)) }*

카드사는 TID, CAVV 쌍을 복호화하고 카드사에서 인증한 코드임을 확인한다. 이후 임시 데이터베이스에 저장되어 있는 해당거래의 IP 주소와 사용자와의 통신으로 전송받은 IP 주소를 비교하여 로그인에 사용된 IP 와 동일한지 확인한후 최종결제 승인과정을 진행한다.

10) Payment_Success { Result || TID }

최종 결제를 진행한 카드사는 연결되어 있는 세션으로 사용자에게는 결제 완료 메시지를 전송하고 PG 사에는 결제완료 메시지와 해당 거래의 TID 를 함께 전송한다

4. 보안성 및 편의성 분석

본 논문에서 제안하는 시스템은 결제를 위해 PG 사에 회원가입시 카드정보를 저장하고 결제 과정에서 추가적인 세션을 이용하여 결제를 진행함으로써 하나의 세션에서 일괄적으로 진행되는 기존 시스템에 비해 우수한 보안성을 가진다. 또한 ISP 인증서나 사용자의 카드번호 입력을 요구하지 않으므로 사용자 편의성도 높아 진다고 할 수 있다. <표 1>은 온라인 전자 결제 시스템에서 발생 가능한 정보 유출을 각 구간별로 나타낸 것이다. 본 단락에서는 표에 나타낸 정보 유출 가능성을 기준으로 제안 시스템의 보안성에 대해 설명한다. 그리고 사용자 편의성 측면에서 기존 시스템의 결제과정과 비교한다.

<표 1> 온라인 결제시스템의 구간별 정보 유출 가능성

온라인 결제 시스템의 구간별 정보 유출 가능성	
PC	■ 악성 프로그램의 키로깅(Key-Logging) ■ 결제 페이지로 위장한 피싱(phising), 파밍(pharming)
가맹점	■ 네트워크 도청(중간자 / 재전송 공격) ■ 데이터의 일시적 복호화로 카드정보 노출
PG / VAN	■ 카드정보 데이터베이스 유출 ■ 네트워크 도청(중간자 / 재전송 공격)
카드사	■ 카드정보 데이터베이스 유출

■ 보안적 측면

1) 악성 프로그램

악성프로그램은 주로 사용자 PC 에 설치되어 사용자가 인지하지 못하는 시점에서 사용자의 정보를 불법적으로 수집한다. 특히 온라인 결제시스템에서는 키로깅(Key-Logging)을 이용한 카드번호의 수집에 취약하다. PC 에 설치된 악성 프로그램은 기존의 Key-in 입력방식이나 안심클릭을 이용하는 사용자가 결제를 위해 카드번호를 입력할 때 악성프로그램으로 카드번호를 유출한다. 제안한 시스템에서는 결제시 카드번호를 입력하지 않으므로 키로깅에 의한 카드번호 유출을 방지 할 수 있다.

2) 피싱 공격

공격자는 사용자를 속이기 위해 실제 결제페이지와 유사한 결제 페이지를 제작/유도 하여 사용자의 정보를 탈취 할 수 있다. 이 같은 경우 사용자 PC 에 악성 프로그램을 설치 하지 않아도 결제에 필요한 정보를 네트워크 통신으로 전송 받을 수 있다. 제안하는 시스템은 로그인을 통한 사용자 인증 진행 후 회원가입시 등록한 이메일 이용한 결제 승인과정을 진행 하므로써 사용자 인증과 동시에 판매자를 인증 가능하게 한다. 사용자가 피싱 사이트에 접속하게 된다면 정상적으로 이메일을 수신하지 못하게 되며 사용자가 직접적으로 카드번호를 입력하지 않는 구조이기 때문에 피싱사이트에 접속한다해도 카드번호는 유출되지 않는다.

3) 중간자 공격

기존 온라인 결제 시스템에서는 사용자-PG 사 사이에 공격자가 위치하여 중간자 공격(Man-in-the-middle attack, MITM)으로 인증 데이터의 변조가 가능하다. 제안 시스템에서는 서비스 인증 세션과 사용자 인증 세션을 분리 함으로써 중간자 공격에 의한 인증데이터 탈취로 인한 부정사용을 방어한다. 이메

일로 전송되어 통신하게 되는 두번째 세션의 경우, 사용자-카드사간 세션으로 사용자-PG 사 에 위치하는 기존의 중간자 공격으로는 거래 데이터를 탈취할 수 없다. 기존 소액결제 시스템에서 SMS 를 이용한 승인코드 발급형태의 경우 악성어플리케이션의 승인코드 탈취를 이용한 부정사용이 발생 가능하다.[13] 제안하는 시스템은 사용자-카드사간 세션에서 승인코드의 대칭키 암호화로 인증 매개변수 전달과 IP 주소를 이용한 이중 인증으로 단순 이메일 전문 탈취로 사용자 인증을 받을 수 없으므로 부정사용에 대응 가능하다.

4) 재전송 공격

공격자가 재전송 공격을 성공시키기 위해서는 사용자의 거래 인증 데이터를 사전에 탈취해야 한다. 제안 시스템은 2 개의 세션을 이용해 데이터 통신을 하므로 공격자가 인증데이터를 탈취하기 어렵고 인증데이터를 수집하더라도 거래에 사용되는 카드정보 매개변수들은 카드사의 공개키로 암호화 되어 있고 타임스탬프 매개변수를 거래에 포함 하고 있기 때문에 재전송 공격이 불가능 하다.

■ 편의적 측면

1) ActiveX 프로그램

기존 온라인 결제 시스템에서 사용자가 가장 거부감을 느끼는 부분 중 하나가 ActiveX 프로그램의 설치이다. 개인방화벽, 키보드 보안 프로그램, 안티백신, 공인인증서 등을 사용하기 위한 목적으로 ActiveX 가 필요하기도 하지만 결제 시스템 자체를 구현하기 위한 프로그램도 설치해야한다. 대부분의 브라우저에서는 로컬파일로의 접근을 보안을 위해 금지 한다. 그러나 ISP 결제의 경우 PC 또는 외장메모리에 저장/접근 하여 ISP 인증서를 불러와야 결제가 가능하므로 ActiveX 프로그램의 설치가 필요하다. 사용자들은 ISP 결제를 이용하기 위해 추가적인 ActiveX 프로그램을 설치해야하고 설치가 완료되도 세션이 만료되어 다시 결제과정을 반복한다. 또한 프로그램의 업데이트시 매번 같은 과정을 반복해야 하므로 사용자들은 큰 불편함을 가지고 있다.

본 논문이 제안하는 시스템은 추가 적인 프로그램의 설치 없이 사용자-PG, 사용자-카드사 간 보안채널 통신을 이용해 결제를 진행하므로 사용자의 편의성도 크게 증가 할 것이다. 또한 추가적인 프로그램을 요구 하지 않으므로 PC 외의 인터넷 활용이 가능한 무선 단말기에서도 활용이 가능하다.

2) 사용자 인증

기존 시스템은 사용자 인증을 위한 수단으로 대표적으로 SMS 를 이용한 본인인증을 사용한다. 본인인증은 사용자 휴대폰으로 인증코드를 전송하고 사용자가 다시 결제 페이지에 입력하는 방식이다. 이러한 방식은 결제를 원하는 사용자와 통신사 가입자의 명의가 동일해가 가능하고 추가적인 단말기기가 필요하다. 이에 반해 제안하는 시스템은 서비스 가입시 인증받은 이메일을 이용한다. 아이디와 비밀번호로 1 차 사용자 인증을 한후 가입시 인증을 받고 등록한 이메일로 링크를 전송하여 결제를 진행하므로 이메일에 접근 권한이 있는 사용자 본인만이 결제를 진행할 수 있다. 또한 로그인한 IP 주소와 이메일 링크를 통해 거래하고자하는 세션의 IP 주소의 대조를 통해 타인에 의한 메일 전문 탈취에도 대응 할 수 있다.

5. 결론

인터넷 전자상거래의 편리함과 접근의 편의성으로 거래 시장의 규모는 해마다 증가하고 있다. 더욱이 모바일 디바이스의 빠른 보급으로 이를 이용한 온라인 전자 결제 시장도 증가 할 것으로 예상된다.

그러나 현재의 온라인 전자결제 시스템은 카드정보나 결제 정보의 유출의 가능성이 크고 시스템의 구조적 문제로 사용자들이 느끼는 불편함이 크다. 이에 본 논문에서는 이메일을 이용한 2-Session 결제 시스템을 제안했다. 제안한 시스템은 추가적인 디바이스를 필요로 하지 않으면서 사용자인증이 가능하고 사용자 입력이나 데이터 통신간 결제정보를 노출 하지 않으면서 거래가 가능하다. 이를 기반으로 기존시스템 대비 향상된 보안성을 가지면서 사용자들의 편의성이 고려된 시스템을 구성하였다.

6. ACKNOWLEDGEMENT

이 논문은 2014 년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2014R1A1B3004161)

참고문헌

[1] 서진호."전자지불서비스 현황 및 ISP/안심결제 도입후 영향분석." 한국통신학회 학술대회논문집 (2005): 1612-1625.

[2] 백은정. “전자지불시스템에서의 구매자 인증강화 방안에 대한연구.” 세종대학교 정보통신대학원(2005)

[3] 김보. “ 전자상거래 지불결제방식(신용카드)의 안전성 분석 및 대응 모델 연구.” 고려대학교 정보경영공학전문대학원(2008)

[4] 임형진, et al. "전자 금융 거래 환경의 인증 기술 동향 분석." 정보보호학회지 18.5 (2008): 84-98.

[5] 박두수, “온라인 소액결제 시스템에서 금융정보 보호를 위한 스마트카드 기반의 프로토콜 설계”, 숭실대학교 대학원(2012).

[6] 황윤성, “클라우드 환경에서의 안전한 모바일 isp 결제 시스템”, 숭실대학교 정보과학대학원(2013)

[7] 유한나, et al. "인터넷 뱅킹 환경에서 사용자 인증 보안을 위한 Two-Channel 인증 방식." 한국통신학회논문지 36.8 (2011): 939-946.

[8] 지은화, 김애영, and 이상호. "USIM 탑재 스마트폰 기반 모바일 신용카드 결제 프로토콜의 안전성 향상." 정보과학회논문지: 컴퓨팅의 실제 및 레터 17.4 (2011): 259-263.

[9] 박인우, and 박대우. "안전결제 시스템의 취약점 및 대응 지침 연구." 정보보호학회지 22.8 (2012): 31-35.

[10] 금융보안 연구원, “전자금융 보안 동향 연구, 2014.12

[11] 금융결제국 전자금융팀, “전자결제 인증체계 개선 방향과 향후 과제”, 2014.5

[12] “3-D Secure: System Overview”, Visa Publication, 70015-01, 2003

[13] “악성코드 분석 보고서”, Red Alert, 2013. 03 05.