情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

안전한 소셜커머스 카드결제 시스템에 관한 연구

허 원 석,† 이 상 진‡
고려대학교 정보보호대학원

Research on Secure Card-Payment System of Social Commerce

Wonseok Heo,† Sangjin Lee‡
Graduate School of Information Security, Korea University

요 약

현재 큰 성장세를 나타내고 있는 소셜커머스 서비스의 전자결제 시스템을 분석한 결과 대부분 결제금액을 변조할 수 있음을 발견하였다. 본 논문은 이러한 카드결제 시스템 상에서 발생하는 금액변조의 문제점을 해결하기 위한 방안을 제안한다. 제안된 방안은 소셜커머스 업체의 서버와 전자결제대행업체 서버간의 검증 체계를 추가하여 구매자가 결제흐름에 관여할 수 없도록 함으로써 결제금액 변조를 원천적으로 막는 방법이다.

ABSTRACT

This paper analyzed electronic transaction systems of social commerce service which have rapidly grown recent days, and as a result found that most of the electronic transaction systems of social commerce service had payment amount modification issue. This paper proposes a method for solving the payment amount modification issue. The proposed method adds an authentication process between servers of social commerce service provider and payment-gateway company. The added authentication process prohibits user getting involved in payment procedure, and thus prevents payment amount modification.

Keywords: Social commerce Card-Payment, Secure Card-Payment System

I. 서 론

전자상거래란 거래 당사자들이 오프라인 공간상에서 거래를 발생시키는 것이 아닌 전자적 방식을 통하여 발생시키는 거래를 의미한다. 과거 물리적 상점 방식을 대체하여 홈페이지로 제작된 온라인 상점 방식으로 전자상거래를 발생시키는 주체의 변화 및 거래방식의 변화가 상거래의 첫 번째 패러다임이었다면, 현물(실물)거래가 아닌 전자태그(상품 바코드, 상품에 부여된 고유번호 등)를 거래하는 것을 상거래의 두 번째 패러다임이라고 말할 수 있다.

접수일(2012년 5월 2일), 수정일(1차 : 2012년 8월 8일, 2차 : 2012년 9월 19일, 3차 : 2012년 10월 25일), 게재확정일(2012년 11월 23일)
† 주저자, beatmk@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr

두 번째 패러다임을 거친 상거래 방식은 아직도 다양한 모습으로 변화를 하고 있다. 다양한 물건을 서로 저렴한 가격에 사고 팔 수 있는 오픈마켓 형태로 시작되었던 초기 인터넷 쇼핑몰이 이제는 TV매체광고(홈쇼핑)와 연동하여 고객 확보를 하는 형태와 소셜 네트워크 서비스(SNS)를 활용한 소셜커머스 서비스 형태로 변화하였다.

이처럼 전자상거래의 모습이 다양하게 변하고 그 규모가 성장할 수 있는 이유는 인터넷이 널리 보급되었기 때문이다. 국내의 경우 가구당 인터넷 보급률이 절반을 넘어선 시점은 2001년부터이며(63.2%), 매년 보급률이 성장하여 2011년에는 81.8% 에 달하였다[1]. 이는 이동통신망을 이용한 무선인터넷에 대한 통계는 제외된 결과이며, 2011년 스마트폰 보급률이 2500만대가 넘은 것으로 보아 현재 인터넷

보급률은 1가구당 100% 이상의 보급률을 나타낸다고 할 수 있다[2].

인터넷 보급률의 증가로 사용자들이 정보를 접할 수 있는 채널(컴퓨터, 스마트폰, IPTV 등)도 증가하게 되었고 따라서 최근 소비자들이 물품 가격, 서비스 품질 등을 인터넷을 통해 쉽게 비교할 수 있게 되다보니 같은 물품을 판매하는 수많은 업체들의 가격 경쟁이 치열하게 되었다. 이렇게 조금 더 저렴한 업체를 찾는 최근 소비자의 경향을 최대한 반영하여 나타난 전자상거래 방식이 바로 "소셜커머스 서비스"이다.

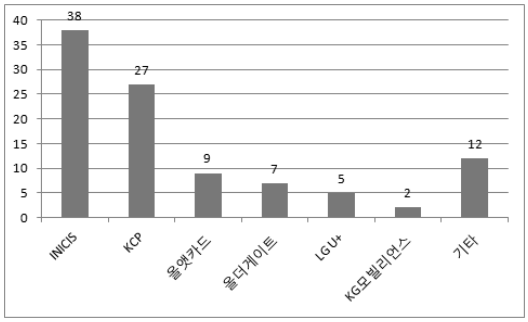
소셜커머스 서비스는 페이스북, 트위터 등의 소셜 네트워크서비스(SNS : Social Network Service)를 활용하여 이루어지는 전자상거래의 일종으로, 일정 수 이상의 구매자가 모일 경우 파격적인 할인가로 상품을 공급하는 전자상거래 방식이다. 기존의 온라인 쇼핑몰은 판매 물품에 대한 수요가 일정하지 않아 납품 업체와의 할인율을 조절하기가 힘든 반면 소셜커머스 서비스는 납품 업체와 판매처가 최소 주문수량을 정하여 그 기준을 만족하게 되면 납품 업체가 기존 할인율에 추가 할인을 제공하기로 계약하는 구조이므로 일정 수 이상의 구매자가 존재하게 되면 구매자는 일반 온라인 쇼핑몰에서 구매 대비 저렴한 가격으로 물품을 구매할 수 있게 된다.

이러한 가격의 이점으로 소비자는 점점 소셜커머스 서비스 제공업체를 선호하게 되었고 소셜커머스 제공업체 또한 증가하게 되었다. 그 결과 2011년 전자상거래 총 거래액이 사상최대인 1000조에 육박하게 되었으며, 그 견인은 소셜커머스 서비스라고 할 수 있다.[3]국내 전자상거래 시장에서 소셜커머스 서비스가 본격적으로 상용화된 시점은 2010년 하반기부터이며, 2012년 3월 현재 개설되어 운영 중인 소셜커머스 사이트의 수는 487개[4]다. 짧은 기간 동안 많은 업체가 무분별하게 양산되다보니 관리적 측면에서 문제점이 발생하였고 이로 인해 공정거래위원회에서는 2010년 11월 26일 소셜커머스 피해주의보를 발령하여 소셜커머스 서비스로 인한 피해를 줄이고자 노력하였다. 이러한 관리적 측면의 시장 안정화 시기가 지나자 2011년에는 시스템 상의 취약점을 이용한 해킹 공격이 발생하기 시작했다. 2011년 6월 쿠팡과 같은 대형 소셜커머스업체의 해킹 사건을 시작으로 소셜커머스업체 시스템을 대상으로 한 크고 작은 사이버 공격들이 발생하기 시작했다. 이에 소셜커머스 업체들은 웹 취약점 공격 등 보안 사고에 대응하고자 보안이 비교적 잘되어 있는 IDC에서 시스템을 운영하고, 보안 컨설팅 등의 방법을 통해 웹페이지의 취약점 등을 많이 해소하고자 노력하고 있다. 하지만 아직 해결되지 않은 문제점이 존재한다. 그것은 소셜커머스 서비스의 카드결제 트랜잭션에 대한 부분이며, 이는 카드결제 트랜잭션의 구조적 문제로 인해 공격자는 구매 물품을 원하는 가격으로 결제할 수 있는 문제를 말한다.

본 논문에서는 웹 변조 취약점 해킹 기법으로 인해 발생하는 소셜커머스 사이트의 가격 변조에 대한 문제점을 취약한 코드 패치 또는 암호화 방법이 아닌 소셜커머스업체와 결제대행업체(PG사) 사이에 결제금액에 대한 검증 체계를 추가하여 보안성이 향상된 카드결제 트랜잭션의 구조를 제시한다.

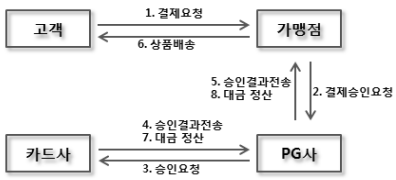
II. 소셜커머스 업체의 카드결제 시스템 사용 현황

금융위원회에 전자금융업자로 등록된 국내 결제대행업체(PG사)는 총 52개사이다[5]. 그 중 상위 3개 업체의 시장 점유율이 78%에 달하며(INICIS : 35%, 한국사이버결제(KCP) 23%, LG U+ 20%), 상위 6개 결제대행업체(INICIS, 한국사이버결제(KCP), 삼성올앳카드, 올더게이트, LG U+, KG모빌리언스)의 시장 점유율은 90% 이상이다.[6]따라서 6개 업체의 전자결제 시스템이 국내 대부분 전자상거래 사이트에 적용된다고 할 수 있다. 현재 소셜커머스 사이트들의 결제대행업체(PG사) 사용 현황 확인 결과 상위 6개 결제대행업체(PG사)의 카드결제 모듈을 사용하는 업체는 88개로 88%의 점유율을 보였으며, [그림 1]은 업체별 점유율을 나타낸다.



[그림 1] 상위 100개 소셜커머스 업체에서 사용 중인 카드결제 시스템 제공 결제대행업체(PG사) 현황(http://banga-banga.com)

상위 6개의 결제대행업체(PG사)에서 말하는 카드결제 트랜잭션은 동일하며, [그림 2]와 같다.



〔그림 2〕 결제대행업체(PG사)에서 제시하는 전자결제 시스템의 카드결제 트랜잭션

하지만 결제대행업체(PG사)에서 말하는 카드결제 트랜잭션과 실제 카드결제 트랜잭션은 약간 상이하다. 결제대행업체(PG사)에서 제공하는 카드결제 구성도를 보면, 구매자가 상점 웹서버로 카드결제 요청을 하는 것으로 되어 있으나 실제 카드결제 트랜잭션은 구매자와 상점 웹서버와 통신하는 것이 아닌 구매자와 결제대행업체(PG사)에서 제공하는 프로그램을 통해 결제대행업체(PG사)로 카드결제 승인요청을 보내게 된다.

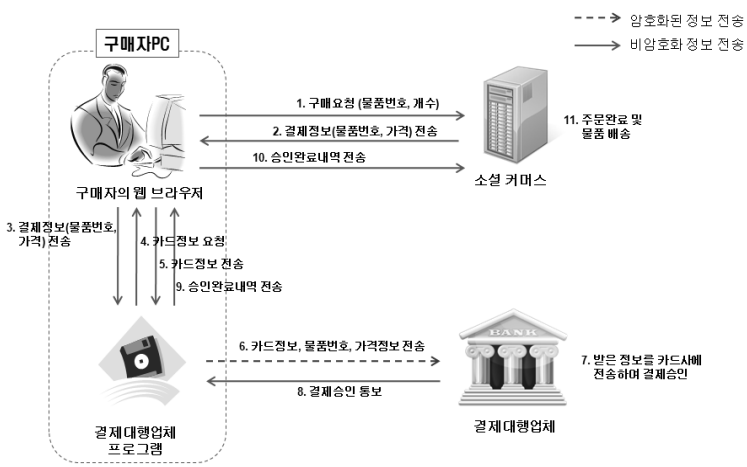
〔그림 3〕은 실제 소셜커머스 웹사이트에서 이루어지는 카드결제 트랜잭션을 나타낸다. 먼저 구매자가 구매하려는 물품을 클릭하면 소셜커머스 서버로 물품번호 및 개수를 요청하게 되며, 이때 소셜커머스 서버는 요청한 정보를 구매자의 웹브라우저로 전송하게 된다. 이후 구매자의 PC에서는 결제대행업체(PG사)의 프로그램을 실행하여 결제대행업체(PG사)의 프로그램에서 물품번호와 가격을 전송받게 되며, 구매자에게 카드정보를 요청하게 된다. 구매자가 카드정보를 결제대행업체(PG사) 프로그램에 전송하면 프로그램은 결제대행업체 서버로 카드정보와 물품번호, 가격정보를 전송하게 되며, 카드사의 승인여부에 따라 정상적으로 결제가 요청되었다면 구매자에게 정상 승인여부를 전송하고 구매자PC에서는 소셜커머스 서버로 승인완료 내역을 전송하게 된다. 승인완료내역을 전송받은 소셜커머스 서버는 주문완료 처리 및 물품배송 안내 메시지를 구매자에게 보내게 된다.

이러한 구조에서 만약 구매자가 자신의 PC에서 결제금액을 변조하면, 결제대행업체(PG사)는 구매자가 결제를 요청하는 요청금액이 정상적인 금액인지 변조된 금액인지 인지할 수 없기 때문에 결제가 진행된다. 다시 말해 구매자가 접근하는 소셜커머스 웹서버에서 웹 취약점에 대한 대응책을 마련해 놓았더라도 결제대행업체(PG사)와 웹서버 사이에 결제금액에 대한 검증 체계가 존재하지 않으므로 결제금액 변조에 대한 문제점이 발생하게 된다.

III. 소셜커머스 카드결제 시스템 결제금액 변조 실험

실험범위는 상위 100개의 소셜커머스 업체이며, 100개의 업체에서 제공하는 전자결제대행 모듈 중 상위 6개의 업체의 모듈과 6개의 소셜커머스 업체를 대상으로 선정하여 카드결제 시 결제금액 변조를 시도하였으며, 실험방법은 아래와 같다.

1) 프록시 도구를 이용하여 프록시 설정 후 소셜커머스 사이트 A에 접속
2) 송수신 데이터를 가로채도록 프록시 도구를 설정하고 구매하고자 하는 물품을 클릭



〔그림 3〕 실제 소셜커머스 전자결제 시스템의 카드결제 트랜잭션

3) 결제금액 부분을 원하는 가격(실험 시 1000원으로 설정)으로 변경을 하면서 결제를 진행
4) 결제금액 변조가 가능하다면 결제금액 변조 가능으로 판단, 그렇지 않을 경우 정상으로 판단
5) 카드승인 시 결제금액을 확인하여 변조된 금액으로 카드승인 시 문제점 존재로 판단, 그렇지 않을 경우 정상으로 판단

실험결과 〔표 1〕과 같이 6개 소셜커머스 업체에서 카드결제 시 결제금액의 변조가 가능하며 승인까지 가능한 것으로 확인되었다.(실험기간 : 2011.10.30~2012.3.30)

〔표 1〕 결제금액 변조 실험 결과 (O : 성공, X : 실패)

소셜커머스 업체	PG사	실험 결과	
		결제금액 변조 가능 여부	금액변조 시 카드승인 가능 여부
A	1	O	O
B	2	O	O
C	3	O	O
D	4	O	O
E	5	O	O
F	6	O	O

〔그림 4〕는 실제 금액변조를 하여 카드결제를 했을 시 결제가 완료된 화면과, 카드사에서 전송해준 SMS 수신 내역이다.

〔그림 4〕의 ①은 구매물품의 정상가격인 6900원을 1000원으로 결제했을 때 소셜커머스 서버에서 금액변조를 인식하지 못하고 구매절차를 정상적으로 완료시켰다는 화면이며, ②는 구매절차가 정상적으로 이루어졌으므로 물품을 배송한다는 안내 SMS 문자 및 구매물품 결제가격이 정상가격 6900원이 아닌 변조된 1000원으로 결제 되었다는 화면이다.

IV. 안전한 소셜커머스 카드결제 트랜잭션 방안 제시

제안하는 안전한 소셜커머스 카드결제 트랜잭션 방안은 '검증 해쉬값을 이용한 카드결제 트랜잭션 구현 방법' 이다. 기존의 카드결제 트랜잭션 방식은 구매물품과 관련된 정보만 존재하는 반면, 구매정보에 대한 해쉬값을 부여하여 부여된 해쉬값의 검증 체계를 추가하게 될 경우 구매자PC에서 결제금액에 대한 변조 여부를 확인할 수 있게 된다. 이유인즉 해쉬값 검증 체계를 소셜커머스사의 서버와 결제대행업체(PG사) 서버 사이에서 구현한다면, 결제금액 변조 여부를 확인하는 과정에서 사용자의 개입이 발생하게 된다면 정상적인 구매정보의 해쉬값과 사용자 개입 후 생성되는 해쉬값이 달라지므로 사용자의 개입이 무의미하게 되므로 구매자PC에서 금액변조에 대한 부분이 무력화된다고 할 수 있다. 아래는 기존 카드결제 트랜잭션과 제안하는 카드결제 트랜잭션에 대한 그림이다.

제안하는 새로운 카드결제 트랜잭션의 내용은 다음과 같다.(TID : 가맹점정보+구매번호+구매물품가격+구매물품갯수에 대한 해쉬값)

1~3) 구매자의 물품구매 요청 발생 시 소셜커머스

〔그림 4〕 1) 소셜커머스 사이트에서 제공하는 물품구매 완료 화면
2) 소셜커머스에서 구매완료 SMS 및 변조된 금액으로 승인된 SMS

서버에서는 구매번호를 부여하여 TID 값을 생성(이하 TIDS)한 후 결제정보(이하 결제정보S)를 구매자에게 전송한다.

4) 구매자는 결제대행업체(PG사)에서 제공하는 프로그램을 실행하여 수신한 결제정보S를 결제대행업체(PG사) 프로그램에 전송한다.

5,6) 결제대행업체(PG사) 프로그램은 전달받은 결제정보S를 복사하여 결제정보C를 생성하고 결제정보C에 대한 TID 값을 생성(이하 TIDC)하여 결제정보C와 TIDC를 결제대행업체(PG사) 서버에 전송한다.

7,8) 결제대행업체(PG사) 서버는 전송받은 결제정보C에서 가맹점정보를 확인하여, 가맹점정보와 일치하는 소셜커머스 서버를 검색하여 해당 소셜커머스 서버에 구매번호를 전송하고 소셜커머스 서버는 구매번호와 일치하는 결제정보S와 TIDS를 결제대행업체 서버에 전송한다.

9) 결제대행업체(PG사) 서버는 소셜커머스 서버에서 전송받은 TIDS와 구매자로부터 전송받은 TIDC의 일치 여부 및 결제정보S와 결제정보C의 일치 여부를 확인하여 정상/이상 거래코드를 생성한다.

10,11) 생성된 정상/이상 거래코드 중 해당되는 거래코드와 구매번호를 소셜커머스 서버에 전송하고 거래코드와 거래번호를 구매자PC의 결제대행업체(PG사) 프로그램에 전송한다.

12) 결제대행업체(PG사) 프로그램은 정상 거래코드일 경우 구매자에게 카드정보를 요청하게 되고, 이상 거래코드일 경우 메시지를 출력 후 카드결제 트랜잭션을 종료한다.

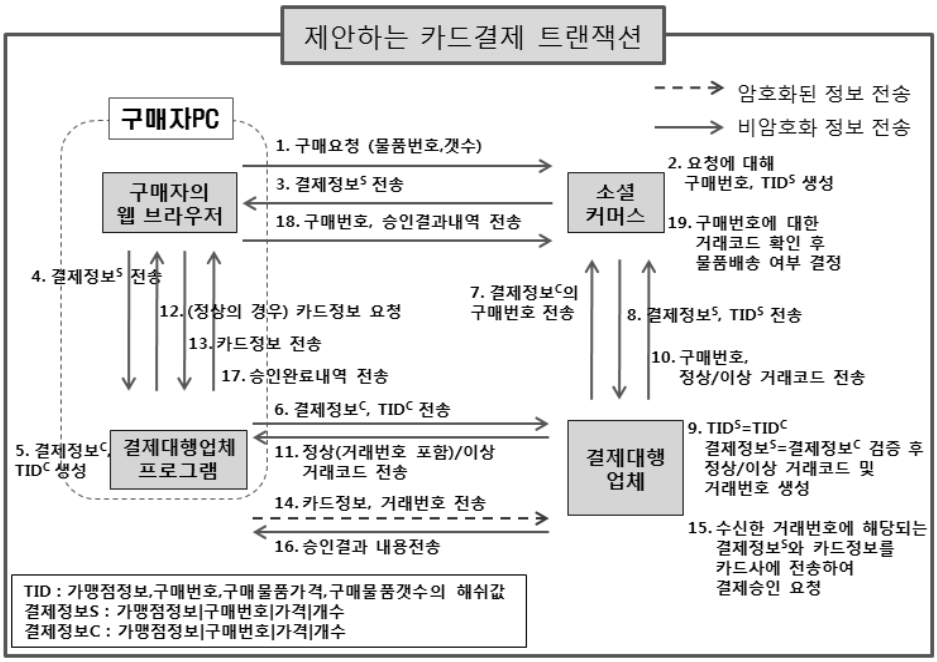
13,4) (정상 거래코드일 경우) 결제대행업체(PG사) 프로그램은 입력받은 카드정보, 결제대행업체(PG사) 서버에서 받은 거래번호를 암호화된 채널로 결제대행업체 서버로 전송한다.

15) 결제대행업체(PG사) 서버는 수신한 거래번호에 해당되는 결제정보S와 카드정보를 카드사에 전송한다.

16~18) 결제대행업체(PG사) 서버는 승인결과 내용을 구매자PC에 전송하며, 구매자PC는 구매번호와 승인결과내역을 소셜커머스 서버에 전송 한다.

19) 소셜커머스 서버는 구매번호에 대한 정상/이상 거래코드를 확인하여 정상 거래코드임이 확인되면 물품배송 준비를 하며, 이상 거래코드일 경우 카드결제 트랜잭션을 종료한다.

제안하는 카드결제 트랜잭션은 두 가지 값(결제정



〔그림 5〕 제안하는 카드결제 트랜잭션

〔표 2〕 기존 카드결제 트랜잭션과 제안하는 카드결제 트랜잭션 비교 내용(- : 해당 없음)

순서	트랜잭션 유형	내용
1	기존	결제정보(가맹점정보, 결제가격)만 구매자에게 전송
	제안	소셜커머스 서버에서 결제정보S(가맹점정보,구매번호,가격,개수)와 결제정보S의 해쉬값인 TIDS를 생성하여 구매자에게 전송
2	기존	결제정보를 결제대행업체 프로그램에 전송
	제안	동일
3	기존	-
	제안	결제대행업체 프로그램은 전달받은 결제정보S를 복제하여 결제정보C를 생성하고 결제정보C의 해쉬값인 TIDC를 생성하여 이 결제정보C와 TIDC를 결제대행업체 서버에 전송
4	기존	-
	제안	결제대행업체 서버는 전송받은 결제정보C의 가맹점정보를 확인하여 해당 소셜커머스 서버에 결제정보C의 구매번호를 전송하며, 소셜커머스 서버는 수신한 구매번호에 해당되는 결제정보S, TIDS를 결제대행업체 서버에 전송
5	기존	-
	제안	결제대행업체 서버는 구매자(결제대행업체 프로그램)로부터 전송받은 결제정보C, TIDC와 소셜커머스 서버로부터 전송받은 결제정보S, TIDS의 일치여부를 확인
6	기존	-
	제안	일치여부 확인 후 소셜커머스 서버에 구매번호, 정상/이상 거래코드 전송 · 정상일 경우 : 카드결제 트랜잭션 계속(정상거래코드, 거래번호(생성) 전송) · 이상일 경우 : 카드결제 트랜잭션 종료(이상거래코드 전송)
7	기존	결제대행업체 프로그램은 카드정보를 구매자로부터 수신 후 카드정보, 결제정보를 결제대행업체 서버로 전송
	제안	결제대행업체 프로그램은 카드정보를 구매자로부터 수신 후 카드정보와 부여받은 거래번호를 결제대행업체 서버로 전송
8	기존	카드정보, 결제정보를 카드사에 전송하여 승인 요청
	제안	카드정보, 거래번호에 해당되는 결제정보S를 카드사에 전송하여 승인 요청

보, TID)를 추가하여 검증하는 방법이 특징이다. 기존의 카드결제 트랜잭션은 결제 시 중요데이터인 가격정보를 평문으로 전송하고 이에 대한 추가적인 검증절차가 없으므로 가격정보의 변조 시 변조된 가격으로 결제가 이루어지는 문제점이 존재하는 반면, 제안하는 방법은 〔그림 5〕의 9)단계에서 결제정보와 TID를 검증하게 되므로 결제가격이 변조가 되더라도 변조여부를 탐지가 가능하므로 정상/이상 거래유무를 판별할 수 있게 된다. 〔표 2〕는 〔그림 5〕에 대해 기존의 카드결제 트랜잭션과 제안하는 카드결제 트랜잭션을 비교한 내용이다.

〔표 3〕은 제안하는 카드결제 트랜잭션의 핵심인 두 가지 검증 값을 추가할 경우 보안성이 향상되는지 여부를 기존 방식과 제안하는 방식의 위변조 취약점에 대한 보안성을 5개 항목으로 검증한 내용이다. 검증결과 위변조 취약점에 노출되는 부분은 기존 방식 1건, 제안하는 방식 0건으로 확인 되었으며, 위변조 취약점을 방어할 수 있는 부분은 기존 방식이 1건, 제안하는 방식은 5건으로 확인되었다. 따라서 제안하는 방식인 두 가지 검증 값을 이용한 카드결제 트랜잭션 구현 방법은 기존 방식에 비해 보안성이 향상된 방법이라고 할 수 있다.

V. 결론 및 향후 연구 과제

본 논문에서는 소셜커머스 사이트에서 카드결제를 함에 있어서 금액변조가 가능한 현재 카드결제 시스템을 분석하고 소셜커머스 서버와 결제대행업체(PG사) 서버간의 검증 체계를 추가하여 금액변조에 대한 문제점을 해결할 수 있는 방안을 제시하였다. 이는 단순히 웹사이트 코드상의 수정으로 인한 보안 패치를 하는 보안 적용 방안에 비해 근본적인 해결 방안을 제시했다는데 의의가 있다.

현재 소셜커머스업체와 결제대행업체(PG사)의 수는 각각 487개와 52개이다. 소셜커머스 사이트의 카드결제 금액변조 부분을 보안할 수 있는 방법 중 웹사

〔표 3〕 제안하는 카드결제 트랜잭션에 대한 검증사항 (O : 양호, X : 미흡, - : 해당없음)

번호	변조 내용	비교대상	검증내용	
			기존 방식	제안하는 방식(모두 양호함)
1	구매자가 전송받은 결제정보c(금액)를 변조할 경우	결제정보(금액)	X	결제정보s(금액) ≠ 결제정보c(금액) 이므로 결제프로세스 종료
2	구매자가 결제대행업체(PG사)에서 배포하는 프로그램의 해쉬 알고리즘을 분석하여 TIDc를 변조할 경우	TID 해쉬값	-	TIDs ≠ TIDc 이므로 결제프로세스 종료
3	구매자가 결제정보c(금액) 변조 및 해쉬 알고리즘을 분석하여 TIDc를 변조할 경우	결제정보, TID 해쉬값	-	결제정보s(금액) ≠ 결제정보c(금액) TIDs ≠ TIDc 이므로 결제프로세스 종료
4	구매자가 승인결과 내용(미승인)을 승인완료 내용으로 변조할 경우	소셜커머스 서버에 저장되는 거래코드	O	구매번호에 해당되는 거래코드가 이상거래 코드이므로 결제프로세스 종료
5	구매자가 물품A는 구매가격이 1000원으로 결제단계까지 진행한 웹브라우저A, 물품B는 구매가격이 2000원으로 결제단계까지 진행한 웹브라우저B 이렇게 두 개의 예비 결제 단계를 만들어 소셜커머스 서버가 구매번호A,B를 생성하도록 하고 웹브라우저B를 통해 결제정보a(구매번호A)와 TIDa을 승인받아(결제금액 1000원) 물품B를 정상 결제한 것처럼 위장할 경우	소셜커머스 서버에 저장되는 거래코드	-	구매번호에 해당되는 거래코드가 없으므로 결제프로세스 종료

이트의 웹소스 수정의 경우 가장 단기간에 해결할 수 있는 방안이지만 웹소스 전체를 다 확인해서 수정해야 하며, 일부 우량한 소셜커머스업체를 제외한 대부분 영세한 소셜커머스업체는 보안담당자가 별도로 지정되어 있지 않기 때문에 웹소스 수정에 대한 방안을 제시한다고 하더라도 487개의 소셜커머스업체 모두가 일시 적용이 어려운게 사실이다. 그렇기 때문에 해당 웹취약점에 대한 보안 적용이 완료되었다고 생각하지만 실제로 몇몇 영세한 소셜커머스 사에서는 문제점이 남게 될 가능성이 농후하다.

또 다른 보안 대책인 구간 암호화 방법의 경우 보안성 향상 측면에서 좋은 보안 대책이지만 결제대행업체(PG사)에서 제공하는 프로그램과 소셜커머스 서버가 세션생성 및 공유해야 하는 부분에 있어서 데이터 암·복호화 시스템, 암·복호화 과정에서 발생하는 트래픽에 대한 비용이 적지 않아 대부분이 소상공인(SOHO)인 소셜커머스업계에서는 투자비용에 대한 부담이 큰 방법이라고 할 수 있다.

이에 비해 제시한 검증 체계 방안을 적용할 경우 소셜커머스업체는 건별 결제정보에 대한 해쉬값 생성(소프트웨어로 가능), 결제대행업체(PG사)에서 요청하는 결제정보와 해쉬값 전송, 구매번호에 해당되는 거래의 정상 유무 확인의 역할을 하게 된다. 이는 암호화 통신을 위한 시스템 구축이 추가적으로 필요하지 않으며, 네트워크 트래픽에 대한 부담감 또한 암호화 방법에 비해 적게 되므로 영세한 소셜커머스업체는 추가적인 비용이 발생하지 않게 되는 이점이 있다. 결제대행업체(PG사)의 입장에서는 배포하는 프로그램에서 해쉬값을 생성하는 알고리즘 추가 및 구매자와 소셜커머스 서버에서 전송받은 결제정보와, 해쉬값에 대한 검증의 추가가 필요하게 된다. 해쉬값 생성 알고리즘 추가는 기존 결제대행 프로그램에 알고리즘 생성 모듈을 삽입하면, 추가적인 프로그램 배포가 발생하지 않게 되므로 웹소스의 수정을 하지 않아도 되고 또한 해쉬 알고리즘은 쉽게 적용할 수 있는 SHA-1과 같은 표준 알고리즘이 존재한다. 검증 부분은 단순히 수신받은 값들에 대해서 동일성 유무만 체크하여 결과에 대한 정상거래 또는 비정상거래 코드만 소셜커머스 서버에 전송하는 내용을 추가하면 된다.

이처럼 제안하는 방법은 단계가 다소 복잡할 수 있고 트래픽량이 크게 증가하지 않을까 하는 우려가 있을 수 있으나 추가 구현하는 내용들이 모두 단순하고 잘 알려진 기술들에 대한 조합이고 TID 해쉬값이 두 번 전송되는 정도의 트래픽만 추가 발생하므로 소셜커머스업체와 결제대행업체(PG사)의 입장에서는 비용적, 시간적 측면에서 여타 보안성 향상 방안에 비해 효과적일 것으로 판단된다.

본 논문에서는 보안성 향상 및 도입에 대한 유연함

을 기반으로 둔 소셜커머스 서비스의 카드결제 시스템에 대한 보안 대응 체계를 제안하였으나 제안한 대응 체계는 기존의 카드결제 트랜잭션에 비해 복잡한 통신 절차를 갖고 있으므로 이에 대한 최적화, 해쉬값 생성 부분에 있어서 더 효율적인 방법에 대해 연구가 이루어진다면, 제안한 보안 대응 체계에 비해 보다 신속하고 효율적인 카드결제 시스템의 보안 대응 체계가 나타날 것으로 생각한다.

참고문헌

〔1〕 방송통신위원회 및 한국인터넷진흥원, 2011년 인터넷이용실태조사, 인터넷통계보고서, pp. 63, 2012년 1월

〔2〕 마케팅인사이트, "〔12-02호〕금년 하반기 스마트폰 보급률 80%에 이를 듯", pp. 3, 2012년 3월

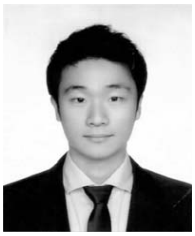
〔3〕 우기종, "2011년 4분기 전자상거래 및 사이버쇼핑 동향 보도자료", 통계청, pp. 7, 2012년 3월

〔4〕 소셜커머스모음 방가반가 전체업체 메뉴, http://banga-banga.com/

〔5〕 "전자금융업 등록 및 말소 현황", 금융위원회, 2012년 2월

〔6〕 오경택, "한국사이버결제(060250) 전자결제 서비스 업체의 가치 발견", 동양종합금융증권, pp. 7, 2011년 6월

〈著者紹介〉



허 원 석 (WonSeok Heo) 정회원
2009년 2월: 인제대학교 컴퓨터공학과 졸업
2009년 3월~2012년 1월: 금융보안연구원 연구원
2009년 2월~현재: 고려대학교 정보보호대학원 석사과정
2012년 1월~현재: 대검찰청 사이버범죄수사단
〈관심분야〉 정보보호, 디지털포렌식, 소프트웨어 보안성 평가, 사이버 법률

이 상 진 (Sangjin Lee) 종신회원
1994년 9월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: 한국전자통신연구원 선임연구원
2006년 2월~2011년 12월: 암호연구회 위원장
2006월 1월~현재: 한국디지털포렌식학회 이사
2008년 3월~현재:고려대학교 정보보호연구원 디지털포렌식센터장
現 고려대학교 정보보호대학원 교수
〈관심분야〉 암호이론, 디지털포렌식