情 報 保 護 學 會 誌
第22卷 第8號, 2012. 12

안전결제 시스템의 취약점 및 대응 지침 연구

박 인 우*, 박 대 우 **

요 약

안전결제 시스템(ISP)의 사고 건수는 2007년 5천만원부터 2010년 1억7천만원, 최근인 2012년 1억 8천만원으로 증가하고 있다. 안전결제 시스템은 국내 최초의 PKI기반 전자서명방식을 적용한 신용카드 인터넷 결제서비스 이다. 안전결제 시스템에 대한 해킹사고가 국민에게 직접적인 금전 피해를 야기 시켜서 사고에 대한 취약점 분석 및 대응 지침에 관한 연구가 필요하다. 본 논문에서는 안전결제 시스템에 대해 정의하고 원리를 파악하여 취약점을 기술하고 분석하여 취약점에 따른 대응 지침을 연구한다. 아울러 국가와 국민의 사이버 안전을 보호하고, 국민들에게 보다 안전하고 편리하게 온라인 결제를 할 수 있도록 하는 연구가 될 것이며 미흡한 온라인 보안 강화를 위한 전자상거래법 개정안이 채택되는데 도움이 될 것이다.

Ⅰ. 서 론

지난 2007년 시티은행에서 20여 명 명의로 5천여만원이 무단으로 결제된 사건이 있었다. 이로 인해 개인 컴퓨터가 해킹된 것으로 드러난 적이 있었다[1].

작년인 2010년에도 신한과 삼성, 현대, 롯데카드 등 4개 사에서 130명 명의로 1억 7천만 원이 무단으로 결제된 사례가 있었지만, 역시 개인 컴퓨터 해킹이었다[2].

더불어 최근인 2012년에도 BC카드와 국민카드의 안심결제 시스템에서 8백30여 차례에 걸쳐 아이템 구매 등으로 1억 8천만 원이 결제되어 조사되는 사건이 발생했다[3].

이와 같이 안전결제 시스템에 대한 해킹공격으로 인한 피해사례가 점점 늘어나고 있으며, 특히 개인정보보호법 시행에 따른 개인정보의 보호를 위해서 안전결제 시스템의 취약점을 분석 및 대응지침의 연구가 필요하다.

본 논문에서는 보안강화를 위해 시행되고 있는 안전결제 시스템의 취약점을 분석하고 해킹공격방법에 대해 알아본다. 그리고 이를 분석하여 안전결제 시스템의 취약점에 대한 대응 지침 방안을 연구한다.

Ⅱ. 안전결제 시스템

현재 보안 강화 대책으로 시행되고 있는 안전결제 시스템의 정의, 원리에 대해 연구한다.

즉, 안전결제 시스템을 조사하고 이를 분석하였다.

2.1. 안전결제 시스템의 정의

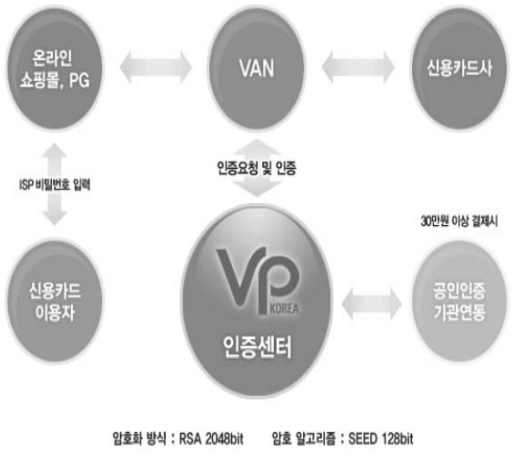
인터넷 안전결제 시스템이란 종전 전자상거래시 신용카드회원께서 신용카드번호 비밀번호 등을 입력함으로써 발생 될 수 있는 개인정보 유출의 문제점을 해소하고 인터넷 안전결제 비밀번호만으로 거래함으로써 안전하고 편리한 전자상거래를 이용할 수 있도록 개발한 국내 최초의 PKI기반 전자서명방식을 적용한 신용카드 인터넷 전용 지불수단 이다[4]. 또한 인터넷 쇼핑몰에서 사용하는 안전하고 편리한 전자인증 및 지불수단으로 무료로 받아서 사용 할 수 있으며 30만원 미만의 소량의 금액을 온라인상으로 결제할 때 주로 이루어지고 있는 결제 서비스 이다.

* 호서대학교 벤처전문대학원(cowboyiw@hanmail.net)
** 호서대학교 벤처전문대학원(prof_pdw@naver.com)

〔그림 1〕 안전결제 시스템 화면

2.2. 안전결제 시스템의 원리

안전결제 시스템은 2008년 5월에 국내 특허를 취득하였으며, X.509 v3 표준형식의 전자인증서 방식을 사용하며 RSA2048bite, 3-DES128bit, SEED, SHA1 등의 고도의 암호화 방식을 가진다. 또한 카드번호, 유효기한 등 카드정보 노출을 차단할 수 있는 End to End 보안방식을 사용하며 거래인증 및 승인을 동시에 진행할 수 있도록 해주는 단일 결제프로세스를 할 수 있다[5]. 그림 2와 같은 원리로 과정을 거쳐 결제 된다.



〔그림 2〕 안전결제 시스템 원리

Ⅲ. 안전결제 시스템의 취약점 분석

안전결제 시스템의 취약점을 조사하고 각 취약점에 대해 분석하고 연구하였다.

3.1. 안전결제 시스템의 취약점

안전결제 시스템은 일반 웹브라우저를 사용하는 결제창과는 달리 별개의 창을 띄우기 때문에 중간에서 결제정보를 탈취하기 어렵기 때문에 비밀번호 자체를 키로깅 등의 수법을 이용해 해킹공격이 가능하다. 또한 안전결제 시스템 특성상 필요한 인증서와 인증서 비밀번호는 당사자 동의없이 카드사에서 불필요하게 저장되며, 고객 본인확인절차가 허술한 상태에서 카드 정보만 알고 있으면 사용자의 동의 없이 재발급이 가능하다는 취약점이 있다[6].

또한 인터넷 뱅킹의 경우 재발급시 기존 인증서가 폐기되지만, 안전결제 시스템은 인증서가 폐기되지 않아 누군가 자신의 인증서를 재발급 받아 사용하는지 여부를 본인이 알 수 없게 돼 있다[7].

표 1은 국내외 카드 결제 시 필요한 정보를 나타낸 표이다. 보안이 많이 취약함을 알 수 있다.

〔표 1〕 국내외 카드 결제시 필요 정보

구분	결제 방식	필요한 정보	비고
국내	VISA 안심클릭	카드번호, 유효기간, 안심클릭 비밀번호	안심클릭 비밀번호 최초 등록시 카드 정보(카드번호, 유효기간, CVC, 비밀번호), 주민등록번호가 필요
	BC ISP 결제	ISP, ISP 비밀번호	ISP 발급/재발급 시 카드 정보(카드번호, 유효기간, CVC, 비밀번호) 필요
	휴대폰 결제	휴대폰 번호 / 통신망 사업자(KT, SKT, LGT)	휴대폰에 문자 메시지로 전송된 임의의 문자열을 요구
국외	PAYPAL	Paypal ID, Paypal Password	고액 거래를 위해선 카드를 거래내역에서 확인해야하는 임의의 문자열을 요구 (첫 고액 거래 시 한 번)
	일반 카드 결제	이름, 카드 정보(카드번호, 유효기간, CVC)	

3.2. 안전결제 시스템의 취약점 분석

인터넷 소액결제에 사용되는 안전결제 시스템도 해커의 공격에 안전치 않아 PC사용자들이 각별한 주의를 기울여야 한다.

안전결제 시스템은 30만원 미만 인터넷 소액결제에 사용되는 결제시스템으로 공인인증서와는 별도로 ISP 인증서를 필요로 하기 때문에 이 ISP인증서와 비밀번호만 알고 있으면 해커들이 손쉽게 다른 사람의 소액결제를 악용할 수 있다.

일반 웹브라우저를 사용하는 결제창과 달리 안전결제 시스템 방식은 별개의 창을 띄우기 때문에 중간에서 결제정보를 탈취하기 어렵기 때문에 비밀번호 자체를 키로깅 등의 수법을 이용해 탈취 가능하다[8].

또한, 국외 결제 시스템과는 달리 ActiveX의 문제점을 알면서도 안정성 때문에 사용하고 있는 카드사에도 문제가 있다. 표 2는 국내 외 결제 시스템을 비교분석해 놓은 것이다.

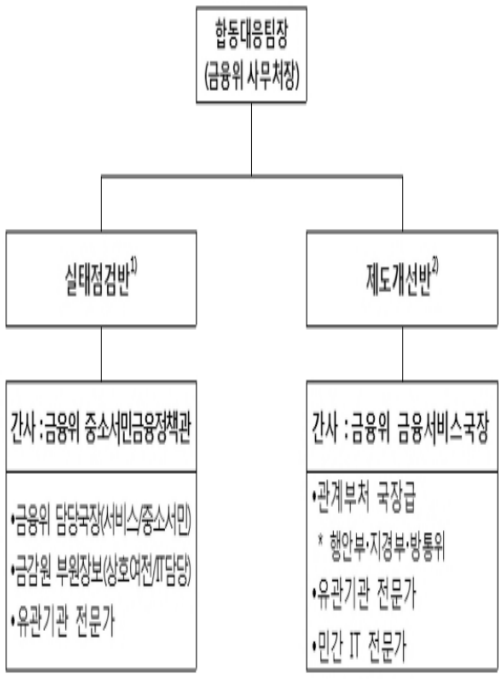
〔표 2〕 국내외 결제시스템 비교

구분	국내	국외
보안 채널	Plugin(ActiveX) 기반	브라우저 내장 SSL 기반
결제창	새 창으로 띄움, 프레임 사용	사이트 내에 임베딩, 프레임 사용 안함
기타	고액 거래시 공인인증서 요구 키보드 보안, 안티 바이러스, 피싱 방지 등을 목적으로 다양한 ActiveX를 필수적으로 설치함	사이트에 따라 결제 주소(Billing address)로만 배송해 주는 경우가 있음

Ⅳ. 안전결제 시스템의 대응 방안

4.1. 정부측 대응 방안

금융당국이 최근 발생하고 있는 '안전결제' 시스템 해킹을 계기로 그림 3과 같이 온라인 결제 보안을 강화한다. 금융위원회는 6일 금융위 사무처장을 팀장으로 행정안전부, 지식경제부, 방송통신위원회 등 관계부처와 민간 정보통신(IT) 전문가, 관계기관, 업계 등이 모두 참여하는 그림과 같이 합동대응팀을 운영하여 안전결제



〔그림 3〕 정부에서 결성한 합동대응팀

시스템 안심클릭 등 온라인 결제 전반의 운영실태와 온라인 거래의 보안을 강화한다. 또한 법령개정 및 제도개선을 위해 제도적 미비점을 보완하고 전자금융법 개정안을 통과될 수 있도록 전자금융거래법 개정안을 국회에 제출한 상태이다.

〔표 3〕 보안 강화 대책 방향

분야	주요 내용
온라인 결제 보안	-ISP/ 안심클릭 결제방식의 보안관리 실태 점검-해외 결제시스템 사례, 제도/기술적 미비점·개선방안 점검
인터넷·모바일 뱅킹& 트레이딩	-공인인증시스템의 안전성 점검-새로운 모바일 수단(스마트폰·태블릿PC 등)의 보안취약점 점검
금융IT 사고 예방/책임 강화	-CEO의 매년 정보보호계획 자필 서명·확인-전 금융회사의 CISO(최고정보보호책임자) 지정 의무화-금융사고 즉시 보고(과태료), CEO제재 감경 폐지(제재규정 개정)
금융회사 IT 인력/예산 강화	-임직원 5%는 IT인력(그중 5%보안인력), IT예산 7%-미충족시 매년 홈페이지 공시 의무화(내년1월부터 시행)-준수한 회사는 감독원 IT실태평가시 우대
금융회사 자발적 점검 상시화	-스스로 매년 취약점 분석·평가(현재는 외부평가기관에 맡기는 관행화)-감독당국은 랜덤 (이행)점검하여 우대 또는 개선명령·제재
IT 검사·감독 강화	-감독원 IT실태평가(종합검사/분기, 부문검사/수시)+IT실태평가 4등급(5등급중) 이하인 금융회사는 경영실태평가 2등급이상 불가-감독원 보안성심의(전산실 신규설치 등 특별한 경우)

4.2. 카드사측 대응 방안

최근 발생하고 있는 안전결제 시스템의 해킹사고에 대해 카드사의 경우, 피해회원에 대해서는 전액 보상하는 걸로 대응 방안을 취했다. BC카드와 국민카드가 제공하는 안전결제 시스템 서비스도 지난 21일부터 보다 강화된 본인인증 절차를 시행했다. 이에 따라 ISP인증서를 사용하던 PC가 아닌 다른 PC로 옮겨 사용하기 위해 복사를 하려면 기존에 카드번호와 ISP비밀번호만으로도 가능했던 것이 카드번호, ISP비밀번호는 물론 카드비밀번호, CVC번호, 주민등록번호 등을 추가로 입력해야 한다. 또 IP도 추가하게 됐다. 이와 함께 결제나 인증 시 입력오류가 3회 발생될 경우 해당 인증서를 삭제하고 재발급을 받도록 했다. 또한 안전결제를 이용해 결제할 때 결제금액 액수에 관계없이 모든 건에 대해 공인인증서 추가 결제를 의무화해서 대처한다.

4.3. 고객측 대응 방안

고객은 안전결제 시스템에만 너무 의존하지 말고 온라인 결제시에 아무리 작은 금액이라도 본인인증을 철저히 하여야 하고, 개인 PC에 백신프로그램을 설치하여 악성코드 및 바이러스에 대해 검사를 해야한다.

Ⅵ. 결 론

안전결제에 대한 해킹공격 피해사례가 발생하고 있고, 보안 수준이 높다고 평가 받았던 안전결제 시스템의 취약점을 조사하고 이를 위한 대응 지침을 연구하였다. 그리고 미국과 우리나라의 결제방식에 대해 비교하여 안전결제 시스템의 취약점에 대한 대응 지침을 연구하였다.

향후 연구에서는 우리나라에서 현재 실행되고 있는 ActiveX의 취약점을 분석하여 SSL을 적용해 암호화를 하거나 더 보안을 강화할만한 인증절차를 연구하여야 할 것이다.

참고문헌

[1] YTN뉴스, "혹시 내 카드도?---'BC,국민'카드, 무단 결제돼", http://m.ytn.co.kr/view_main.php?s_mcd=0103&key=201212041421110705, 2007년.

[2] 뉴스 ZUM, "BC,국민카드 소액결제 해킹 수사“ http://webcache.googleusercontent.com/search?q=cache:EE9reOaWVUcJ:news.zum.com/articles/4696524+2010%EB%85%84+%EC%B9%B4%EB%93%9C+1%EC%96%B5+7%EC%B2%9C%EB%A7%8C&cd=14&hl=ko&ct=clnk&gl=kr, 2010년.

[3] 서울신문, “국민,BC카드 ISP해킹 수사 190명 1억8000만원 피해”, http://www.seoul.co.kr/news/newsView.php?id=20121205010009, 2012년

[4] KISA, '인터넷 침해사고 동향 및 분석월보', 2012년 10월.

[5] KISA, '인터넷 침해사고 동향 및 분석월보', 2012년 9월.

[6] KISA, '인터넷 침해사고 동향 및 분석월보', 2012년 8월.

[7] KISA, '인터넷 침해사고 동향 및 분석월보', 2012년 7월.

[8] KISA, '인터넷 침해사고 동향 및 분석월보', 2012년 1월.

〈著者紹介〉

박 인 우 (In-Woo Park)
정회원

2012년 2월 : 호서대학교 정보보호학과 졸업 <공학사>
2012년 9월 : 호서대학교 벤처전문대학원 융합공학과 (정보보호전공)
2012년 9월 ~ 현재 : 호서대학교 벤처전문대학원 융합공학과 석사과정
<관심분야> 정보보호, 추적기법, Hacking, Forensic, 스마트폰 및 이동단말 보안

박 대 우 (Dea-Woo Park)
종신회원

1998년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
2004년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
2004년 2월 : 숭실대학교 겸임교수
2006년 2월 : 정보보호진흥원 (KISA) 선임연구원
2007년 3월 ~ 현재 : 호서대학교 벤처전문대학원 교수
<관심분야> Hacking, CERT/CC, 침해사고대응, e-Discovery, Forensic, 사이버국방, 정보보호, 유비쿼터스 네트워크 보안, WiBro 보안, VoIP보안, 스마트폰 및 이동단말 보안