스마트폰과 전자상거래

이동산 | 페이게이트 이사

1. 스마트폰이란?

스마트폰과 전자상거래를 이야기하기 앞서 스마트폰의 정의에 대해서 짚어 보자. 아이폰은 국내에서 처음 대중화된 스마트폰이다. 여기에 경쟁하기 위하여 안드로이드폰이나 윈도우7폰, 블랙베리폰 등 다양한 스마트폰이 출시되었거나 출시 예정으로 있다. 그런데 우리 주변에는 스마트폰 외에도 다양한 네트워크된 기기들이 존재한다. 전자책 단말, IPTV, 넷북, 카 내비게이터, 게임기 등이 이미 출시된 네트워크화된 기기들이고 향후 미래에 출시될 다양한 이종 복합기기들도 역시 스마트폰이 가지고 있는 대표적인 특성을 가지고 있다. 대표적인 특성이란 웹(Web)을 의미한다. 웹 브라우저는 대부분의 신종 기기에 기본 탑재되어 있고 이에 기반한 기술발전이 지속적으로 이루어지고 있다. 순수웹(PureWeb) 환경에서 동작하는 서비스라면 이러한 신종기기에서도 여전히 동작가능함을 보장할 수 있다. 즉 스마트폰은 순수웹으로 대표되는 표준환경을 상징적으로 나타내는 아이콘이라고 할 수 있다.

2. PC와 스마트폰 전자상거래 환경의 차이점

한국 내에서 스마트폰 전자상거래가 중요한 이유는 PC 전자상거래가 바이너리 플러그인(Binary Plugin)에 의존한 기형적 환경으로 발전해왔기 때문이다. ActiveX로 대표되는 바이너리 플러그인은 PC 전자상거래에서 중요한 역할을 하고 있다. 대표적으로 공인인증서 전자서명 생성이나, 키보드보안, 안티바이러스, 팝업제어 등 다양한 역할을 수행한다. 그런데 이러한 바이너리 플러그인이 스마트폰으로 대표되는 순수웹 환경에서는 동작하지 않는데서 문제가 발생한다. 스마트폰에서 전자상거래를 한다는 의미는 웹표준 전자상거래와 동일한 의미를 가진다. 스마트폰처럼 새로운 기기가 나타날때마다 요즘처럼 야단법석을 떨면서 대응방안을 마련해야 할까? 필자가 속한 회사에서는 2007년부터 미국 애플사의 온라인스토어에 대한 결제서비스를 웹표준 환경에서 제공하고 있다. 이후 아이팟터치, 아이폰 등이 출시되었고 아이패드도 출시 예정이다. 그런데 애플 온라인스토어는 신종 기기 출시에 따른 결제문제에 대해서 걱정이 없다. 웹표준 환경에서 동작하는 결제 인프라를 갖추었고 이는 자사 단말뿐만 아니라 경쟁사 단말에서도 온라인스토어는 정상적으로 서비스될 수 있다는것을 "당연히" 알고 있기 때문이다.

3. 전자상거래 결제수단

스마트폰 전자상거래에 대해서 본격 이야기하기 전에 온라인에서 이용가능한 주요 결제수단이 어떤 것들이 있는지 살펴보자. 대표적으로 신용카드, 무통장 입금, 계좌이체, 휴대폰결제 등이 많이 사용되고 있다.

결제수단	특징
신용카드	· 자신의 신용카드로 결제대금 지불 · 전 세계적으로 가장 많이 사용
무통장 입금	· 결제대금을 나중에 지급할 것을 통지 · 비 실시간 · 나중에 지정된 은행계좌에 입금하는 형태
실시간 계좌이체	· 자신의 은행계좌이체 실시간으로 결제대금 이체
휴대폰결제	· 이동통신사 청구서에 결제대금이 포함되도록 이통사를 통해 결제 · 월 결제가능 금액이 적어서 소액에 주로 사용

이러한 결제수단 중 무통장 입금이나 휴대폰결제 등은 현행 스마트폰에서 결제하는 데 제도적인 장애가 거의 없어서 임시적인 조치로 많이 사용되고 있다. 그러나 가장 많이 이용되는 신용카드나 실시간 계좌이체 등은 해결해야 할 다양한 이슈들이 존재하여 현재 본격적으로 스마트폰에서 이용되지 않고 있다.

4. 신용카드 전자상거래 체계

신용카드는 전자상거래에서 가장 많이 사용되는 결제수단이다. 기본적으로 신용카드 결제체계에서 이용되는 용어에 대해서 알아보자.

- 카드발행사: 신용카드를 발행하는 카드사를 의미하며 우리가 통상 알고 있는 은행이나 카드사가 여기에 해당함
- 카드브랜드: 신용카드는 특정 브랜드를 가지고 발급됨. 비자, 마스터 등이 익히 알고 있는 카드브랜드이고 카드발행사에서는 브랜드사와 제휴하여 국제 브랜드에서 구축한 네트워크를 이용함
- 카드매입사: 신용카드 거래발생 후 가맹점에게 대금을 지급하는 카드사. 국내거래에서는 카드발행사가 곧 카드매입사인 경우가 대부분이지만 해외거래에서는 카드발행사와 카드매입사가 구분됨

해외의 경우 통상 가맹점은 특정 매입사와 계약하면 해당 매입사가 취급하는 모든 브랜드를 거래처리할 수 있다. 즉 A카드에서 발행한 A 비자카드라면 A카드는 카드발행사이고 비자는 카드브랜드를 의미한다.

국내에서는 카드 브랜드와 관계없이 대표 매입사 약 8개 사와 각각 계약체결을 해야만 국내에서 발행된 모든 신용카드를 처리할 수 있다. 각 카드사별로 전자상거래 결제방식이 조금씩 다르고 거래조건도 다르기 때문에 중소 쇼핑몰이 각 카드사별로 직접 계약하여 전자상거래 시스템을 구축하기보다는 결제대행사를 통하여 쇼핑몰을 운영하는 것이 비용대비 훨씬 효율적이다.

4.1 글로벌 전자상거래

전자상거래는 온라인이라는 특성상 국경의 제약이 없다. 국내 머천트가 해외 구매자에게 상품을 판매하거나 해외 머천트가 국내 구매자에게 상품을 판매하는 등의 행위가 자유롭게 이루어진다. 해외의 유명한 대형 결제대행업체 또는 머천트로는 PayPal, Amazon, eBay, Alipay, Apple, WorldPay 등이 거론되며 이런 업체들은 전 세계를 대상으로 자신의 상품이나 서비스를 판매한다. 국내에 들어와 있는 대표적인 머천트로 애플을 들 수 있다.

국내 유저들이 애플 AppStore에서 애플리케이션을 구매하여 다운로드 받을 때는 해외 금융기관을 통해서 거래처리가 되며 실제 국내 금융관련 규제를 받고 있지 않

다. 예를 들어 30만 원 이상 가격의 애플리케이션을 국내 유저가 공인인증서 없이 자유롭게 구매할 수 있다. 또한 국내 유저가 아마존에서 도서나 전자제품을 구매할 때도 마찬가지고 한국 내의 전자상거래관련 금융규제를 받지 않고 있다.

5. 전자상거래 보안

국내에서 바이너리 플러그인(Binary Plugin) 기반의 전자상거래가 확산된 것은 보안성을 향상시키기 위한 측면이 크다. 그러나 보안 시스템을 클라이언트 환경에 대한 과도한 제어에 집착하여 웹 애플리케이션 보안에 집중하지 못한 이유로 스마트폰 환경에서는 기존 보안체계를 가져갈 수 없는 문제에 봉착하였다. 스마트폰 전자상거래에서의 보안은 웹 애플리케이션 보안과 일맥상통한다.

전 세계적인 보안흐름은 단위 보안 기술에 집착하기보다는 전자상거래 Player의 총체적인 보안체계를 향상시키기 위하여 노력하고 있다. 국제적인 보안 요구사항은 방화벽 등으로 대변되는 네트워크보안뿐만 아니라 보안관리를 위한 업무분장이나 변화관리체계 그리고 웹 애플리케이션 보안을 위한 소스검증, OWASP 대응, 웹방화벽, 외부 취약점 스캐닝, 모니터링 등 총체적인 정보보호 체계를 갖추도록 요구한다.

국제적인 신용카드 브랜드사들은 3D Secure 같은 단위 카드인증방식에서 발전하여 PCIDSS(Payment Card Industury Data Security Standard) 등과 보안규정을 제정하고 이를 준수하도록 가맹점에 요구하는데 이러한 보안 요구사항은 철저하게 순수웹(PureWeb)환경에서의 웹 애플리케이션 보안에 집중하고 있다.

6. 모바일웹과 앱

모바일웹(Web)과 앱(App)은 PC에서 순수웹과 바이너리 플러그인과의 관계와 비교해볼 수 있다. 모바일에서의 웹과 PC 환경에서의 순수웹은 사실상 동일한 웹이며 개발자의 의지에 따라 제한없는 기술구현이 가능한것은 모바일에서는 앱이고 PC에서는 바이너리 플러그인이다.

특히 앱은 주로 스마트폰 등에서 구현되는 개념이며 앞서 이야기한 광의의 스마트폰 환경에서는 앱의 설치나 동작자체가 불가능하다. 공인인증서를 이용한 전자서명 생성 등을 앱을 이용해 구현할 수 있지만 전자상거래 인프라를 앱에 의존했을 때는 다음과 같은 치명적인 약점을 가진다.

앱의 해외벤더 의존성	· 앱을 등록하고 취소하는 전권을 해외벤더가 가지고 있고 해외벤더가 앱 등록을 안해주거나 승인취소해버릴 가능성이 비지니스 리스크로 존재함
앱 피싱 (Phishing) 위험	· 웹에서 앱을 호출할 때 의도하지 않은 다른 앱이 호출될 기술적 가능성이 존재함 · 다른 앱이 악의적인 앱이라면 중요한 개인정보가 빠져나갈 가능성이 존재함
앱 개발 유지의 어려움	· 다양한 플랫폼이 지속적으로 나오고 플랫폼의 운용체제도 버전이 계속 업데이트되는데 이때마다 앱을 신규개발하거나 버전에 맞추어 수정해야하는 문제 발생

전자상거래 인프라를 모바일웹 기반으로 구축했을 때는 웹을 기반으로한 결제서비스뿐만 아니라 하이브리드 애플리케이션 형태로도 앱 내에 웹 패널을 내장하여 결제서비스를 이용할 수 있다. 그런데 현재 국내 금융규제를 그대로 따르게 되면 애플리케이션 형태로는 스마트폰 결제를 할 수 있지만 모바일웹으로는 결제가 불가능하다.

7. 어떠한 제도적 장애요인들이 있고 어떻게 극복할 수 있을까?

7.1 공인인증

전자금융거래에서 30만 원 이상 거래금액일 때 공인인증서를 사용해야 한다. 공인인증서 사용의 의미는 거래내역에 대한 전자서명을 하라는 의미이고 전자서명은 순수웹(PureWeb) 환경에서는 현행 기술규격으로는 가능하지 않다. 공인인증서의 발급/재발급/갱신은 PC의 ActiveX를 통해서만 가능하며 공인인증서의 저장위치도 KISA에서는 NPKI Folder 등 브라우저에서 인식하지 못하는 특정 위치를 지정하고 있으며 저장형식 역시 PKCS#8 포맷으로 SEED 암호화하여 저장하도록 요구한다. 그리고 이러한 공인인증서 사용을 전자금융거래시 금융위에서는 사용을 강제하고 있다. 이 모든 규정을 준수하기 위해서는 스마트폰에서는 앱을 이용하는 것 말고는 대안이 없어 보인다. 그러나 스마트폰 환경에서의 공인인증서 사용를 위해서 이미 다양한 해법이 모색되고 있다. 공인인증서 발급시 서버에서 KeyPair를 생성하여 이용하고자 하는 Client로 내려보내는 방식, 공인인증서 저장위치는 브라우저가 인식할 수 있는 브라우저나 OS 내장 KeyStore에 저장, 저장형식 역시 PKCS#8 포맷이나 PKCS#12로도 저장할 수 있도록 허용 및 전자금융 거래 시 공인인증서를 사용강제하지 않고 공인인증서 사용이 불가할 경우 다른 대안을 선택할 수 있도록 허용하는 것 등이 해법이다.

구분	현행규정	해법	관계기관
공인인증서 발급/재발급/갱신	MS Windows IE 환경에서 ActiveX 이용	서버에서 Key Pair를 생성하여 Client로 내려보냄	KISA
공인인증서 저장위치	NPKI폴더등 브라우저에서 인식하지 못하는 위치	브라우저 내장 KeyStore에 저장	KISA
공인인증서 저장형식	SEED 암호화된 PKCS#8 포맷	PKCS#12 format	KISA
공인인증서 사용	30만 원 이상 모든 전자금융거래 시 사용강제	공인인증서 사용불가환경에서는 다른 대안(SSL+OTP 등) 선택 허용	금융감독위원회

현행 규정과 해법을 다음과 같이 정리해 보았다.

공인인증서가 훌륭한 기술이고 현재 광범위하게 확산되어 있어 국가적으로는 매우 훌륭한 자산임은 분명하다. 기술적으로는 현행 이용형태를 지속적으로 개선해 나가지만 광의의 스마트폰 개념에서 공인인증서를 사용할 수 없는 환경은 항상 존재하며 이러한 갭(Gap)은 미래에도 영원히 지속될 수 밖에 없다. 공인인증서를 사용할 수 없는 환경에서는 다른 대안을 선택해서 사용할 수 있도록 허용하는 것이 스마트폰 전자상거래 문제를 해결하기 위해서 매우 중요하다. 공인인증서를 사용할 수 없는 환경의 기준이 매우 모호할 수 있으나 필자가 제시하는 해법은 "공인인증기관이 인증서를 발급하는 환경"은 공인인증 의무사용 범위로 정하고 그 외의 환경은 다른 대안을 선택할 수 있도록 허용한다는 것이다. 공인인증기관은 지속적으로 다양한 환경에서 인증서를 발급하고 사용할 수 있도록 개선해 나간다면 공인인증 의무사용 범위는 자연스럽게 확대될 수 있으며 그 외의 환경은 사업자의 선택에 따라 다른 기술적 대안을 이용할 수 있다.

7.2 기술적 오용

PC환경에서 바이너리 플러그인(Binary Plugin)을 사용하면서 축적된 기술적 오용이 스마트폰 전자상거래에 장애가 되는 요소가 있다. 대표적으로 iframe이나 오토 팝업(auto popup) 제어 문제를 들 수 있다. iframe은 바이너리 플러그인을 적용하기 위해 주로 이용하는데 목적은 사이트 방문 유저들에게 플러그인 설치를 강제하기 위해서 iframe을 이용하는 것이다. 그런데 이것이 기본적인 접속자체를 불가능하게 하는 경우가 많다.

유저는 단순히 사이트를 조회하기 위해서 방문하는 것이지만 혹시 플러그인이 사용될 가능성에 대비하여 미리 플러그인 설치를 요구하는 형태에서 비롯되었다. 기존 바이너리 플러그인을 이용한 전자상거래 방식

과 스마트폰 전자상거래의 조화로운 공존을 위해서는 iframe을 사용하는 형태는 배제하고 innerHTML을 이용하는 것이 적절하다. 바이너리 플러그인을 갑자기 버릴 수는 없다면 그것이 꼭 필요할 때 동작가능한 환경에서만 잠깐 활성화하여 이용하는 것이 조화로운 해법이다. 그러기 위해서는 바이너리 플러그인을 동적으로 호출하는 코드를 innerHTML에 생성하여 이용할 수 있다.

오토 팝업은 스팸 등에 의한 이용자 피해를 막기 위해서 대부분의 브라우저에서 기본으로 차단하게 되는데 전자상거래 결제방식 중에서 안심클릭 결제방식은 팝업에 의존하여 결제를 진행하기에 오토 팝업 제어가 중요한 이슈이다. 기존 PC에서는 결제 팝업은 허용되도록 하기 위해서 역시 바이러니 플러그인이 사용되는데 웹 표준환경에서의 기술적 해법은 유저 팝업(user popup)을 이용하는 것이다. 유저 팝업은 유저가 명시적으로 팝업을 오픈하는 행위를 하는 경우 차단하지 않는다는 오토 팝업에 대응한 기술적인 브라우저 벤더의 해법이며 스마트폰을 포함한 모든 웹 표준브라우저 환경에서 이용가능한 기술적 대안이다.

보안서버 구축 역시 또 다른 기술적 오용의 대표적 사례이다. 전송데이터 보호를 위해서 보안서버를 구축하는데 법률에서는 바이러니 플러그인을 이용한 방식과 SSL 방식 2가지를 모두 허용하고 있다. 보안서버 구축을 바이러니 플러그인을 통해서 하게 되면 스마트폰에서의 접근은 원천적으로 차단되며 유일한 선택은 SSL을 이용하는 것이다. 기술적 오용에 대한 현황과 대안을 다음과 같이 정리하였다.

구분	현행	대안
바이너리 플러그인 배포	iframe을 이용하여 site 전역에 걸쳐 최초 접속 시부터 플러그인 설치 강제	innerHTML 내에 플러그인 설치 코드를 동적으로 생성하여 이용
오토 팝업 제어	바이너리 플러그인을 이용하여 오토 팝업 제어	유저 팝업으로 전환하여 유저가 명시적으로 팝업오픈 행위를 하도록 유도하여 팝업제어
보안서버 구축	바이너리 플러그인 이용 또는 SSL	SSL만을 이용

7.3 키보드보안, 안티바이러스, 개인방화벽

전자금융거래법 시행세칙 29조에서 요구하고 있는 사항 중에서 키보드보안, 안티바이러스 및 개인방화벽 소프트웨어를 설치하도록 하고 있다. 대다수 전자상거래 사이트에서 전자결제를 진행할 때 위 언급된 기능을 위해서 바이러니 플러그인이 사용되고 있다. 그런데 실제로는 꼭 플러그인을 이용하지 않더라도 위 요구사항을 달성할 수 있다. 금융감독원에서는 스마트폰 카드결제 보안대책 문서에서 용어를 입력정보 보호대책, 악성코드 예방대책과 같이 변경했다.

입력정보 보호대책은 플러그인을 탈피했을 때 다양한 보호방식을 함께 사용할 수 있다. 자바스크립트을 이용한 화면 키보드, OTP 이용 및 브라우저 auto form filler기능 등을 함께 이용하는 경우 충분하게 입력정보를 보호할 수 있다. 악성코드 예방은 통상 안티바이러스 프로그램을 먼저 떠올리지만 모바일웹 환경에서는 웹 애플리케이션에 대한 보호대책이 악성코드 예방대책으로 적용가능하다. OWASP 10대 보안취약점 대응 코드 리뷰하고 수정, 웹방화벽, 정기적 침투시험 등 웹 애플리케이션 보호를 위한 모든 보호대책이 악성코드 예방대책으로 이용된다. 현행 규정과 대안을 다음과 같이 요약했다.

구분	현행	대안
입력정보 보호대책	키보드보안 바이너리 플러그인	· 자바스크립트 화면키보드, OTP, 브라우저 Auto Form Filler 활성화 등
악성코드 예방대책	안티바이러스 바이너리 플러그인	· OWASP 10대 보안취약점 대응 코드 리뷰 및 수정 · 웹 방화벽, 정기적 침투시험 등 웹 애플리케이션 보호를 위한 모든 보안방식

8. 보안성 심의

전자금융거래법에 의하면 전자금융업자가 기존에 존재하지 않았던 새로운 플랫폼이나 새로운 결제방식을 도입하는 경우 보안성 심의를 득하도록 요구한다. 보안성 심의는 결제서비스가 보안상 안전한지를 살펴보는 것을 위주로 하는데 문제는 공무원이나 해당 소속 기관의 이해범위 내에서만 서비스를 허용한다는 데 있다. 금융감독원은 결코 보안 전문 집단이 아니다. 비보안 그룹에서 최신 IT기술에 기반한 서비스의 보안성을 심의하고 서비스 허용 여부를 결정하는 것은 분명한 한계가 있다. 또한 보안성 심의 요청 자체를 대형 금융기관을 통해서 1차 검증받은 이후 금감원에 심의요청하도록 요구하는데 대형 금융기관은 보안성 그 자체보다는 자사 이익에 부합되는지 여부를 먼저 따져서 보안성 심의를 요청할 것인지 결정한다. 즉 비 보안 요소에 대한 비지니스적인 결정 이후 보안성 심의요청 여부를 결정하는데 그에 따라 중소 IT서비스 기업의 서비스 기회자체를 박탈하게 되는 부작용이 존재하며 법에 명시된 대로 보안 그 자체에 대해서 전자금융업자라면 그 규모에 관계없이 누구든 보안성 심의를 요청할 수 있도록 규등한 기회가 부여되어야 한다.

9. 맺음말

아이폰으로 인해 촉발된 스마트폰 전자결제 문제는 기존의 제도나 기술의 불합리성이 부각되는 계기가 되었다. 그러나 지금까지 쌓아왔던 기술적 자산이나 법률을 무시할 수 있는 것은 결코 아니다. 특히 공인인증 인프라는 다른 나라에서는 가지고 있지 않은 대한민국의 특별한 자산이라고 평가하며 다양한 환경에서 잘 활용될 수 있도록 꾸준하게 개선을 추구해야한다. 그리고 새로운 환경이나 서비스가 또한 과거의 유산에 의해 제한되지 않고 민간의 창의적 자율성이 보장받을 수 있는 조화로운 공존이 가능한 환경이 되기를 기대해본다. TTA

정보통신용어해설

웹키트

WebKit [컴퓨터]

웹 브라우저를 만드는 데 기반을 제공하는 레이아웃 엔진.
웹키트는 원래 맥 오에스 텐의 사파리 웹 브라우저 엔진으로 사용하기 위해 컨커러 브라우저의 KHTML 소프트웨어 라이브러리에서 가져온 것이었으나 최근에는 애플의 사파리(Safari)와 구글 크롬(Chrome)은 물론 림의 블랙베리에서도 브라우저의 엔진으로 사용되고 있다.