情 報 保 護 學 會 誌
第23卷 第1號, 2013. 2

스마트폰을 활용한 안전한 온라인 승인시스템 연구

진 승 만*

요 약

최근 전자상거래 및 전자금융 기술이 크게 발전하면서 관련기술이 비약적으로 발전하고 있다. 하지만, 편리성 측면의 기술발전이 빠르게 이뤄지는 반면, 안전성측면의 기술발전은 이를 지원하지 못하는 측면이 있다. 실제, 거래가 증가함에 따라 금융정보 등을 유출하는 등의 보안사고도 증가하고 있음이 이를 반증하고 있다. 이러한 기술적인 문제를 해결하고자 다양한 보안 솔루션이 제공되었지만 보안 솔루션의 보안기능이 강화될수록 다양한 환경에서의 이용자 편의성이 저하되어 스마트폰 등과 같은 신기술 시장의 활성화를 저해하는 요인이 되고 있다. 따라서 본 논문에서는 현재 전자상거래에서 발생되는 보안위협을 살펴보고 발생된 보안위협을 최소화하면서 단말기에 설치된 OS 또는 브라우저에 종속되지 않는 보안기술을 제안한다. 제안한 보안기술은 이미지를 이용한 인증기술로서 별도의 보안 프로그램이 불필요하기 때문에 보안기술로 인해 제한되는 서비스가 발생되지 않아 다양한 환경에서 활용될 수 있으며, 이로 인해 이용자는 보다 안전하고 다양한 서비스 환경에서 전자상거래 및 전자금융거래를 수행할 수 있다.

Ⅰ. 서 론

최근 옥션과 인터파크, G마켓 등 온라인 쇼핑몰을 포함한 지급 결제 금액은 55조원에 달하고 있으며 한국은행의 자료에 따르면 지난해 비금융기관의 지급결제 이용금액이 54조7000억 원으로 전년대비 19.7% 증가하였고 이 중 온라인 지급 결제를 중계하는 전자지급결제 대행 금액이 대부분을 차지하였다. 이는 온라인 쇼핑과 같은 인터넷 상의 거래가 큰 폭으로 급증하고 있음을 증명하고 있으며 최근 들어 스마트폰 시장과 응용서비스가 확대됨에 따라 장소에 구애받지 않고 스마트폰을 이용한 상품을 구매하는 모바일 쇼핑 시장 등의 전자상거래가 확대될 것으로 전망되고 있다. 향후 전망으로 국내에서 G마켓 등과 같은 오픈마켓 거래 전용 애플리케이션을 개발하여 온라인 쇼핑이 가능해질 것이며, 신용카드와 계좌이체, 휴대전화 등의 결제 수단을 스마트폰에서도 사용할 수 있을 것으로 예상하고 있다. 이와 같이 신기술 등장에 따른 이용자의 편의성과 활성화를 위해 앞으로도 다양한 매체에서 전자상거래가 활성화될 것으로 예상됨에 따라 온라인 결제를 통한 보안상의 위협과 위험 또한 지속적으로 증가할 것으로 예상된다.

최근 들어 온라인 결제 시스템에 대한 여러 차례 해킹 사건 발생과 다양한 보안 위협이 발표되면서 금융당국과 금융회사들은 강화된 보안정책과 보안 솔루션을 이용하여 이용자 금융 정보보호 활동을 강화하고 있지만 이에 대응하는 해커들의 수법 역시 점점 다양해지고 있다. 그 예로 최근까지 4개 신용카드사의 안심결제를 통해 발생한 부정결제 피해는 약 1800여건으로 알려졌고, 국내 인터넷 쇼핑몰 219개 사이트를 해킹해 결제 계좌번호를 자신들이 확보해 놓은 계좌 번호로 변경하여 상품대금을 가로채는 등의 사건이 발생하였다. 이러한 국내환경 하에 본격적인 스마트폰 시장이 활성화 되면서 PC에서 했던 온라인 쇼핑을 언제 어디서든 이용할 수 있게 되었는데, 이는 스마트폰의 기능과 성능 그리고 다양한 어플리케이션의 호환성과 확장성에서 기인한 것으로 현재 PC에서 발생되고 있는 보안 위협이 스마트폰에서도 동일하게 적용 되어 위와 유사한 해킹 사건과 보안 위협 출현이 예상된다. 또한 스마트폰의 종류와 플랫폼이 다양하므로 악성코드도 다양한 형태로 나타날 것으로 예상되며 이미 해킹(Jail Break)된 아이폰의 개인 정보를 탈취하는 악성코드가 등장했다. 이에 대한 보안대책을 마련하고자 금융회사들은 보안 솔루션을

* 전북은행 전산정보부 정보보호팀 (smjin7@jbbank.co.kr)

강화하는 등의 대책을 마련하였지만 해커들의 다양한 해킹 수법에 어려움을 겪고 있는 실정이다.

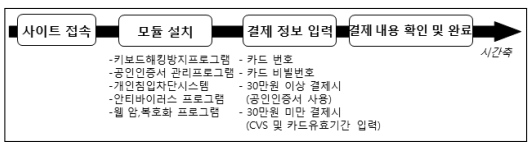
온라인 결제 시스템의 각 요소에서 다양한 위협들이 존재하는데 특히 이용자 단말기에서 발생될 수 있는 위협은 관리적인 측면으로 위협을 제거할 수 없기 때문에 다양한 보안 솔루션을 개발하여 이용자의 금융정보를 보호해야 한다. 현재까지 개발된 보안 솔루션은 지속적으로 발생되는 위협을 차단하기 위해 지속적으로 보완되고 있으나, 이러한 노력에도 불구하고 이용자의 금융정보가 유출되는 상황이 발생되고 있다. 따라서 이용자의 금융정보가 유출되었다면 이와 같은 상황을 이용자는 빠른 시간 내에 감지해야 하고 이용자의 금전적인 손실이 발생되지 않는 것이 중요한 사항일 것이다. 온라인 결제에 있어 가장 보편화된 위협으로는 온라인 결제 시 탈취된 이용자의 금융거래 정보를 이용하여 상품 대금을 결제하고 이용자는 금전적인 손해를 보는 위협이다. 즉 악의적인 자는 취약한 온라인 쇼핑몰에 접속한 이용자가 결제를 수행할 때 이용자의 금융거래 정보를 탈취하고 이를 통해 상품구매를 할 수 있게 된다. 이와 같은 보편적인 위협을 막기 위해 본 논문에서는 결제 매체에 대한 이용자 인증 강화 및 결제 매체 분리 기법을 통해 악의적인 자가 탈취한 이용자의 금융거래 정보를 이용하여 대금을 결제할 수 없도록 온라인 결제 시스템을 구성하였다. 현재의 온라인 결제 시스템에는 입력매체보호, 통신프로토콜 암호화, 데이터 암호화 솔루션 등 이용자 금융 정보보호를 위해 다양한 보안 솔루션들이 지속적으로 개발되고 있으며 이용자의 PC 환경뿐만 아닌 스마트폰 등과 같은 이기종 매체에서도 동일한 보안성을 유지하기 다양한 보안 솔루션 개발과 연구가 이루어지고 있는 중이다. 그러나 현재 국내 이용자 PC 환경에서 온라인 결제 환경에서 적용되어 있는 대부분의 보안기술은 마이크로소프트사에서 제공하는 API를 이용하여 개발한 것으로 솔루션 배포와 동작이 액티브 엑스(ActiveX)를 기반으로 하고 있어 액티브 엑스를 지원하지 않는 스마트폰에 일반 PC 보안수준과 동일 또는 유사한 보안 기술을 적용하기 위해서는 새로운 기술을 개발하는데 필요한 기준이나 시간적인 유예가 요구되고 있다. 이는 이용자PC 뿐만 아니라 스마트폰을 이용한 온라인 결제 시스템의 활성화를 저해하는 요인이 될 것이며 동시에 스마트폰 시장의 확대를 막는 요인으로 충분한 대책이 이루어져야 하며, 현재와 같은 방식으로 하나의 운영체제에 종속적인 보안 솔루션을 개발한다면 스마트폰의 활성화를 기대하기 어렵다. 따라서 다양한 운영체제에서도 적용 가능한 보안 솔루션을 개발하여 여러 가지 운영체제와 환경을 수반하는 스마트폰 환경에서도 안전한 결제를 수행할 수 있을 것이다. II장에서는 현재 온라인 결제 시스템 현황 및 위협에 대해 살펴보고 III장에서는 제안하는 기술인 이기종 매체를 통한 온라인 결제 시스템과 안전성 분석 및 적용 시 고려사항에 대해 살펴본다.

Ⅱ. 온라인 결제 시스템 현황 및 위협

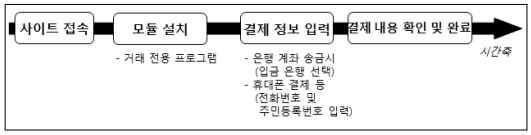
2.1. 온라인 결제 시스템 현황

현재 온라인 결제 시스템은 금액에 따른 차등 결제 방식을 제공하고 있으나 이를 보호하기 위한 보안 강도는 인터넷 뱅킹 등과 같은 전자금융거래 서비스와 동일한 보안강도를 지니고 있다. 온라인 결제 시스템에서 다양한 운영 및 보안 솔루션이 적용되어 있다. 운영 프로그램으로는 주로 전자지불보조사(Payment Gate)에서 제공하는 온라인 결제 관련 프로그램에 해당되며 보안 프로그램으로는 키보드 해킹 방지 프로그램, 공인인증서 프로그램, 웹 암·복호화 프로그램 등이 설치된다. 각 보안 프로그램에서 제공하는 주요 보안기능으로는 키보드 해킹 방지 프로그램으로부터 이용자가 입력하는 결제 정보를 보호하며 공인인증서 프로그램의 경우 이용자 부인방지, 웹 암·복호화 프로그램의 경우 네트워크 채널로 전송되어지는 데이터를 암호화하는 기능을 제공한다. 온라인 결제에 필요한 이용자 환경으로는 주로 윈도우 운영체제와 마이크로소프트사에서 제공하는 인터넷 익스플로러(Internet Explorer) 환경에서 동작하며 액티브 엑스(ActiveX) 기술을 이용하여 솔루션이 배포되고 관리·운영되어지고 있다.

현재 스마트폰을 이용한 온라인 결제 시스템은 이용



〔그림 1〕 이용자PC에서 온라인결제



〔그림 2〕 스마트폰을 이용한 온라인 결제 시스템

자PC와 같이 이용자의 금융거래 정보를 보호하는 솔루션 및 연구가 미흡하여 PC에서 발생되고 금융거래 정보에 대한 유출 위협이 내재되 있다. 즉 키보드 후킹 및 평문 유출 등에 대해 입력값을 보호하는 솔루션 부재로 인해 이용자의 금융거래 정보가 유출될 수 있으며, 거래 정보에 대한 무결성 및 인증을 제공하지 않아 메시지에 대한 위·변조 공격에 취약할 수 있다. 보안 솔루션을 개발하기 앞서 새로운 시장 영역인 만큼 보안적인 측면뿐만 아니라 확장성을 고려해야 할 것이며, 이를 위해 서로 다른 운영체제 또는 브라우저에서 운영 및 보안기능을 적용할 수 있는 방안이 함께 연구되어야 할 것이다.

2.2. 온라인 결제 시스템의 보안 위협

본 절에서는 온라인 결제 시 이용자PC에서 발생될 수 있는 보안위협을 설명한다. 기술될 보안위협은 단순히 이용자PC의 위협으로 국한되지 않는다. 아직까지 스마트폰을 이용한 온라인 결제 시 발생된 보안사고 사례는 없지만 스마트폰 시장의 활성화 및 이를 이용한 온라인 쇼핑의 급성장은 이용자PC와 동일한 보안위협 또는 그 이상의 위협이 존재할 수 있다. 따라서 이용자PC에서 발생된 보안위협은 스마트폰에서 또한 발생될 보안위협으로 보안 전문가들은 이에 대한 연구를 진행 중에 있다.

2.2.1. 결제 입력 정보 노출 위협

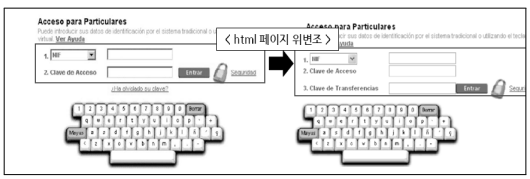
전자금융거래서비스를 사용하기 위해서는 이용자PC에 키보드 해킹 방지 프로그램 등과 같은 입력 보호 프로그램이 반드시 설치되어야 한다. 과거와 달리 현재 키보드 해킹 방지프로그램은 지속적인 보안 강화로 보안성 및 안전성이 매우 향상되어 있다. 하지만 운영체제와 소프트웨어의 한계점으로 인해 고속폴링 취약점, 디버그 레지스트리 조작을 통한 취약점 등 다양한 해킹방식을 통한 키보드 입력값 노출 위험이 지속적으로 거론되고 있다.

〔그림 3〕 DOM 영역을 통한 ID/PASSWORD 절취

현재 이를 대체하기 위한 다양한 매체가 제안되고 있으며 가장 대표적인 기술로는 가상키보드 입력매체를 꼽을 수 있는데, 이러한 프로그램 또한 이용자PC의 자원을 이용하여 방어를 해야 하는 고난위도 기술이 포함되어야 한다. 또한 현재 소액결제 프로그램의 대부분은 인터넷 익스플로러(Internet Explorer)에서 동작되도록 구현되어 있다. 이러한 방식의 경우 해당 페이지에 종단간(End-to-End) 암호화 시스템 또는 이에 준하는 보호 프로그램이 적용되어 있지 않을 경우 메모리 영역 또는 DOM(Document Object Model) 기법에 의해 결재 금액 또는 중요 결제 정보가 노출 될 수 있는 위협이 존재한다.

2.2.2. 피싱 · 파밍에 의한 이용자 결제 정보 절취

웹(Web) 기술을 이용한 온라인 결제 시스템은 피싱 또는 파밍 등과 같은 해킹 기법 등을 이용하여 이용자 결제 정보를 손쉽게 절취할 수 있는 보안 위협이 존재한다. 즉 이메일 또는 잘못된 링크에 의한 결제 정보 입력 페이지의 접근을 유도하거나 혹은 이용자PC를 감염 후 A사이트로부터 전송되어지는 데이터 중 A사이트 결제 페이지와 유사한 B사이트 결제페이지를 전송받도록 변경하여 이용자 결제 정보를 절취하는 보안 위협이 존재한다. 현재 일부 금융사에서 피싱·파밍 방지 프로그램의 설치를 적극 유도하고 있다.



〔그림 4〕 변조된 금융거래 페이지 조작을 통한 금융정보 절취

2.2.3. 액티브엑스(ActiveX)에 의한 이용자PC 권한 상승

소액결제 운영 프로그램 및 보안 프로그램 설치 또는 구동은 마이크로소프트사의 액티브 엑스 기술을 이용하여 이루어진다. 액티브 엑스 기술의 경우 적법한 사업자의 공개키로 배포파일을 서명하고 서명된 배포파일을 이용자가 동의하면 그 이후부터 별다른 질의 없이 해당 프로그램이 이용자 PC의 자원의 접근이 가능하다. 문제는 액티브 엑스 배포에 따른 문제점 보다는 액티브 엑스 응용 기술에 의해 많은 보안 취약점이 노출되고 있다. 가령 잘못된 액티브 엑스 배포 설계로 인해 이용자 PC 내의 정보를 불법 유출 할 수 있는 취약점, 임의 명령을 질의 할 수 있는 취약점, 비정상 호출에 의한 자원 절취 등 많은 취약점 요소가 내포되어 있다. 더욱더 큰 문제는 액티브 엑스 취약점 조치에 있어 대부분의 액티브 엑스 프로그램이 이용자PC에 상시적으로 운영 중인 프로그램이 아니기 때문에 유관 액티브 엑스 프로그램 보안패치가 발표되어도 이에 대한 실시간 적용이 불가능하여 해당 취약점을 조치하기 위해서는 이용자 스스로 액티브 엑스 배포 사이트 또는 별도의 배포파일을 설치하기 전까지 해당 취약점에 이용자PC가 보안 취약점에 지속적으로 노출된다는 점이다.

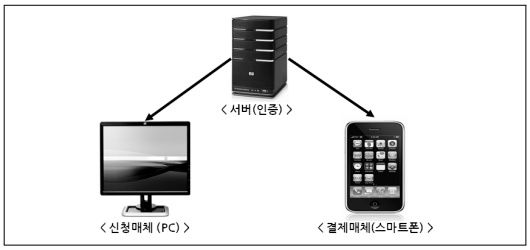
```
<OBJECT ID="update" WIDTH=0 HEIGHT=0
 CLASSID="CLSID:9D01F646-E3C6-4F19-A904-4BC88E9CDE79">
<PARAM NAME="pam1" VALUE="AAAAAAAAAAAAAAAAAA…AAAAA">
</OBJECT>
<script>
        update.UpdateURL = "http://AAAAAAAAAAAAAAAAAAAAAA.....AA";
        update.CreateMenu("type:AAAAAAAAAAAAAAAAAAAAAA…AAAAAAAAA";
</script>
```

〔그림 5〕 액티브엑스 모듈의 취약성을 이용한 사용자 PC 권한 상승

Ⅲ. 이기종 매체를 통한 온라인 결제 시스템

본 장에서는 II장에서 언급한 다양한 보안 위협을 최소화하기 위해 이기종 매체를 연계한 온라인 결제 시스템을 제안한다. 이기종 매체의 경우 최근 이동통신과 정보검색 등 개인 PC 기능이 추가된 지능형 단말기인 스마트폰과 자동 회원가입 방지를 위해 사용되는 캡차[1] 기술을 접목하여 확장성과 보안성이 향상된 온라인 결제 시스템을 설계하였다.

3.1. 시스템 구성요소



〔그림 6〕 시스템 구성 요소

3.1.1. 결제 서버

결제 서버 (이후 서버)는 온라인 결제에 이용되는 매체를 인증하기 위한 데이터(이미지)를 생성하는 구성요소로 정상적인 거래를 승인하는 역할을 수행한다.

3.1.2. 신청 매체

이용자는 온라인 쇼핑을 통해 상품을 결정하고 서버에 결제를 신청하는 매체(예:이용자PC)로 상품정보, 대금 등의 정보를 서버에 전송한다.

3.1.3. 결제 매체

결제가 신청된 상품에 대한 대금 지급을 위해 필요한 매체(예:스마트폰)로서 이용자는 결제에 필요한 금융정보를 입력하는 매체에 해당된다. 결제 매체는 이용자로부터 입력받은 금융정보를 서버에 전송하게 된다.

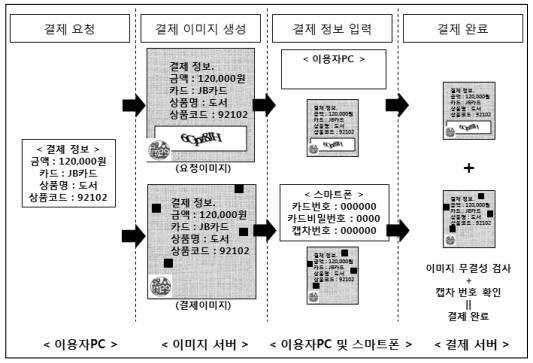
3.2. 전체 서비스 흐름도

3.2.1. 전체 흐름도

기존에 온라인 결제 시스템은 하나의 매체에서 온라인 쇼핑과 지불을 동시에 수행하여 논리적인 방법에 의

1) CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart, 자동가입방지)는 어떠한 사용자가 실제 인간인지 컴퓨터 프로그램인지를 구별하기 위해 사용되는 방법으로, 인간은 구별할 수 있지만 컴퓨터는 구별하기 힘들게 의도적으로 비틀어 놓거나 그림을 주고 그 그림에 쓰여 있는 내용을 물어보는 방법

해 수집된 정보를 손쉽게 악용할 수 있었으나 제안기술은 물리적인 매체를 추가하여 결제를 분리된 매체에서 수행함으로써 악의적인 자의 공격에 대한 성공 확률을 낮추고 보안위협을 최소화하는데 그 목적이 있다. <그림 7>은 이러한 내용을 간략하게 도식화한 그림이다.



〔그림 7〕 전체 흐름도

3.2.2. 결제 이미지 생성

서버는 원본 이미지(임의의 배경 이미지+상품정보)를 생성한다. 그 후 다음과 같이 신청 매체와 결제 매체에 전송할 두 개의 다른 이미지를 생성한다.

가. 신청 매체에 전송될 이미지 생성(이후 요청 이미지) : 원본 이미지(임의의 배경 이미지 + 상품 정보)에 캡차 이미지를 삽입한 이미지 생성

나. 결제 매체에 전송될 이미지 생성(이후 결제 이미지) : 임의의 비트를 스테가노그래피 기법을 이용하여 원본 이미지에 은닉하는 방법으로 삽입한 이미지 생성

생성된 요청 이미지는 결제 신청 매체인 이용자PC에 보내고 결제 이미지는 결제 매체인 스마트폰으로 보낸다.

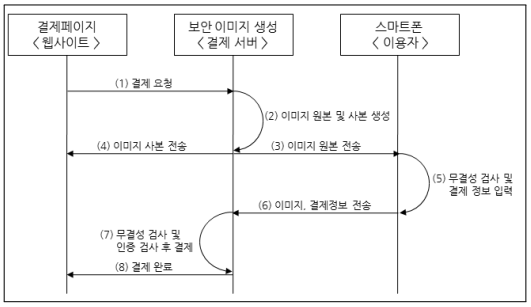
3.2.3. 결제 정보 입력

서버로부터 받은 결제 이미지와 요청 이미지를 이용자는 두 개의 다른 매체에 각각 소유하고 있으며 육안으로 두 이미지에 포함된 정보를 확인한 후 결제 매체에서의 각 입력란에 카드 번호, 카드 비밀번호, 캡차 기술로 생성된 문자열을 입력한다. 이후 입력 정보와 이미지를 다시 이미지와 입력된 거래정보를 암호화하여 서버로 전송한다.

3.2.4. 결제 완료

결제 매체로부터 전송된 이미지에 삽입된 임의의 난수값을 스테가노그래피를 이용하여 추출하고 변조여부를 확인한 후 입력되어진 결제 정보를 이용하여 최종 결제를 완료한다.

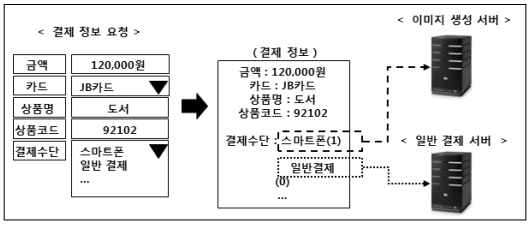
3.3. 제안기술에 대한 세부절차



〔그림 8〕 세부절차

3.3.1. 이용자PC (결제 요청)

이용자는 결제금액, 카드사명, 결제에 필요한 상품코드 등의 결제 정보를 전송한다. (결제수단을 선택할 때 스마트폰을 선택하게 된다면 이용자가 소유하고 있는 스마트폰에서 결제를 수행하게 되고, 일반결제를 선택한다면 보안 프로그램을 설치한 후 결제를 이용자PC에서 수행할 수 있다.)



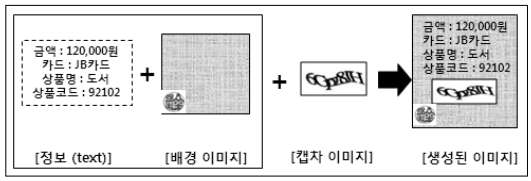
〔그림 9〕 결제 요청

3.3.2 서버 (요청 이미지 및 결제 이미지 생성)

서버는 이용자가 요청한 결제정보를 이용하여 다음

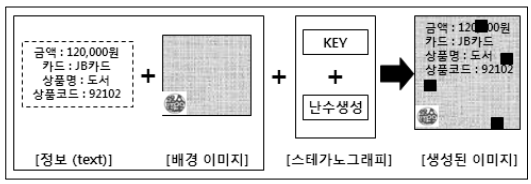
과 같은 이미지를 생성하고 최종 결제 단계 전 이용자 및 결제 정보 확인을 위해 이미지 및 결제 정보를 저장한다.

가. 서버는 원본 이미지(결제 정보+임의의 배경이미지)를 생성한 후 매 세션마다 랜덤하게 생성되는 캡차 이미지를 삽입한 요청 이미지를 생성한다.



〔그림 10〕 요청 이미지 생성

나. 서버는 임의의 난수값을 생성한 후 암호화하여 암호문을 생성한다. 이후 원본 이미지에 스테가노그래피 기법을 이용하여 암호문을 원본 이미지에 은닉한다.



〔그림 11〕 결제 이미지 생성

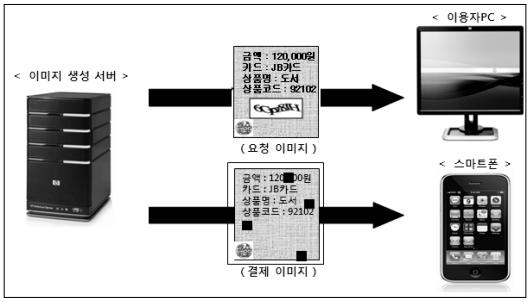
다. 서버는 다음과 같은 결제 정보, 이용자 정보, 보안 정보를 저장한다.

결제 정보	금액	120,000원
	카드종류	JB카드
	상품명	도서
	상품코드	92102
이용자 정보	핸드폰번호	010-1234-1234
보안 정보	캡차 문자열	6GPZI8IH
	이미지 해쉬값	7172A0EAA121F123SS1123
	난수값	dajq3o50relkjgvsdpfiekjrq02
	암호키	1934ekr302ev0ew-1kerjf0s;

〔그림 12〕 서버의 저장 데이터

3.3.3. 서버 (이미지 전송)

서버는 생성된 두 이미지를 신청 매체와 결제 매체에 각각 전송한다. 미리 서버에 등록해 놓은 폰 번호를 통해 생성된 결제 이미지를 스마트폰으로 전송할 수 있다.



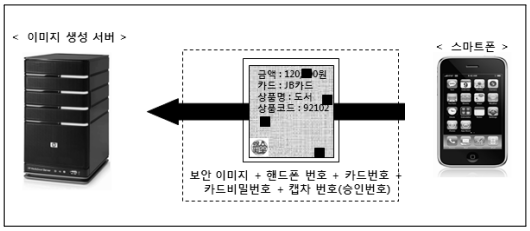
〔그림 13〕 매체 전송 이미지

3.3.4. 이미지 확인 및 결제 정보 입력

이용자는 결제를 수행하기 전 서버로부터 이용자PC로 전송된 요청 이미지와 스마트폰으로 전송된 결제 이미지에서 이용자의 결제 정보를 육안으로 비교한다. 즉 신청 매체로 전송받은 이미지와 결제 매체로 전송 받은 이미지의 차이는 캡차 이미지 이외에 변화가 없음을 확인 할 수 있는데, 만일 배경 이미지나 결제 정보의 변화가 있다면, 피싱이나 파밍에 의해 조작된 결제 정보임을 의심할 수 있다. 두 개의 다른 채널로 전송된 결제 정보를 확인한 이용자가 PC로 전달된 요청 이미지에 표시된 캡차 문자열을 스마트폰에 입력하고, 카드번호 등을 입력 결제에 필요한 결제 정보를 입력한다.

3.3.5. 결제 이미지 및 결제 정보 전송

스마트폰으로 전송된 결제 이미지를 기반으로 다음과 같은 결제에 필요한 정보를 입력 후 이를 암호화하여 서버로 전송한다.



〔그림 14〕 결제 정보 전송

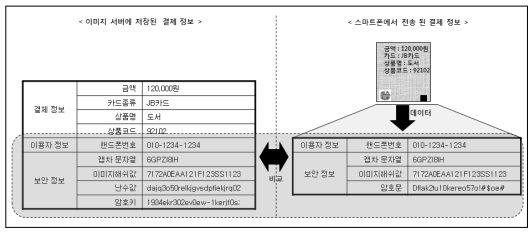
가. 서버로부터 전송되어진 결제 이미지
나. 스마트폰에서 추출한 폰 번호
다. 카드 번호

라. 카드 비밀번호
마. 캡차 문자열(승인번호)

3.3.6. 무결성 검사 및 승인

이용자의 스마트폰에서 전송되어진 결제 이미지와 결제 정보는 최종 승인 전 전송된 데이터의 위·변조를 검사하기 위해 다음 과정을 수행한다.

가. 서버는 스마트폰으로부터 전송된 암호문을 복호화 하여 결제 이미지를 얻는다.
나. 스테가노그래피 기법을 이용하여 결제 이미지로부터 암호문을 추출한 후 복호화 하여 임의값을 얻는다.
다. 스마트폰으로 전송된 폰번호를 이용하여 해당 임의값을 저장된 데이터베이스에서 로딩한 후 두 임의값을 비교한다.



〔그림 15〕 무결성 검증

라. 두 임의값이 동일한 경우, 결제 매체로부터 전송받은 결제 이미지의 해쉬값을 생성하고 서버에 저장된 결제 이미지의 해쉬값을 최종으로 비교하여 그 무결성을 검증한다.
마. 위와 같은 사항에 대해 무결성 검증이 완료되면 마지막으로 캡차 문자열(승인번호)을 마지막으로 비교 후 최종 승인 절차를 완료한다.

Ⅳ. 안전성 분석

4.1. 보안요소

4.1.1. 서버인증

서버는 원본 이미지로부터 변형된 이미지를 생성하여 결제를 신청한 매체와 결제를 수행하는 매체에게 보내게 된다. 이 때 이용자는 서버로부터 받은 신청 매체의 이미지와 결제 매체의 이미지를 육안으로 확인하여 변경된 정보의 유무를 확인할 수 있다. 두 이미지에 삽입된 정보는 이용자가 선택한 정보로서 정상적인 서버만이 두 이미지를 변경 없이 생성할 수 있고 정상적인 이용자에게 보낼 수 있으므로 이용자가 자신의 결제 정보에 대한 유무를 확인함으로서 서버 인증을 수행할 수 있다.

4.1.2. 매체인증

서버는 원본 이미지에 캡차 이미지를 추가하여 변형된 이미지를 신청 매체에 전송한다. 이 때 결제를 수행하는 이용자는 캡차 이미지를 육안으로 확인한 후 결제 매체에서 캡차 이미지 입력란에 문자열을 입력하게 된다. 서버는 전송받은 캡차 문자열 확인을 통해 정상적인 매체에서 보낸 메시지임을 확인한다. 즉 결제를 신청한 이용자와 결제를 수행하고자 하는 이용자가 두 매체를 동시에 소유하고 있음을 서버에서는 확인할 수 있다.

4.1.3. 데이터 암호화

결제 매체에서는 카드관련 정보 및 캡차 문자열을 입력받고 이를 암호화 하여 서버로 전송하게 된다.

4.1.4. 위·변조 방지

서버는 결제 정보의 위·변조를 막기 위해 생성되는 이미지에 임의의 난수값을 은닉하게 된다. 은닉기법으로 스테가노그래피 기법을 이용하며, 임의의 난수값의 유출 방지를 위해 서버는 대칭키 암호화 알고리즘을 이용하여 임의의 난수값을 암호화한다. 생성된 암호문은 결제 이미지에 은닉되어 결제 이미지에 대한 변경을 시도한다면 이후 추출된 임의의 난수값 확인을 통해 결제 정보가 변경되었거나 악의적인 자로부터 보낸 데이터임을 확인하게 된다.

4.2. 위협 시나리오 별 안전성 분석

4.2.1. 서버 가장 공격을 통한 데이터 위·변조

악의적인 자는 악성코드에 감염된 이용자PC로부터

결제 정보를 얻더라도 주요한 금융 정보는 얻을 수 없다. 그 이유로는 제안 기술은 신청 매체와 결제 매체가 분리됨으로서 해킹이 용이한 이용자PC에서 결제에 필요한 금융 정보가 요구되지 않는다. 하지만 악의적인 자는 결제 페이지를 위·변조하여 스마트폰인 결제 매체에 보낼 경우 악의적인 자는 매 세션마다 달라지는 원본이미지(배경이미지, 금액, 상품명 등 포함)를 동일하게 생성해야 한다. 이 때 악의적인 자가 스마트폰(결제 매체)과 이용자 PC(신청 매체)를 동시에 해킹해서 모든 정보를 이용하여 원본이미지를 생성할 지라도 암호화된 임의의 난수값이 삽입된 결제 이미지를 생성할 수 없다. 결제 이미지를 생성하기 위해서는 임의의 난수값, 암호키, 결제 이미지에 삽입된 위치 등을 알아야 생성할 수 있다. 이와 같은 정보는 해킹된 스마트폰이나 이용자PC로부터 얻을 수 없고 단지 서버에만 그 정보가 저장되어 있기 때문에 악의적인 자는 정상적인 요청 이미지와 결제 이미지를 생성할 수 없다.

4.2.2. 매체 가장 공격을 통한 거래정보 위·변조

악의적인 자는 해킹에 용이한 이용자PC로부터 정보를 습득하여 이용자 ID/PW로 로그인 후 온라인 결제를 시도할 경우 서버에 등록된 자신의 스마트폰을 이용하여 결제를 수행해야 한다. 사전에 등록된 결제 매체의 폰번호로 결제 이미지가 전송되기 때문에 정당한 이용자는 자신이 신청하지 않은 상품에 대해 결제가 요청됨을 자신의 스마트폰에 전송된 결제 이미지를 통해 알게 된다. 만일 악의적인 자는 자신의 스마트폰을 이용하여 정상적인 결제 이미지를 받아도 이용자 PC에 전송된 신청 이미지의 캡차 문자열을 알지 못한다면 결제를 더 이상 진행할 수 없다. 즉 기존 결제 방식의 경우 이용자 PC가 피싱·파밍 또는 기타 악성코드 감염에 의해 이용자PC 결제 정보를 절취하고 이를 이용한 결제를 시도할 수 있다. 하지만 본 논문에서는 제안하는 방식으로는 이용자의 결제 정보인 상품, 금액, 카드번호, 카드비밀번호, 캡차 문자열 등 결제 정보가 절취되더라도 승인에 필요한 결제 이미지를 전송 받을 매체(스마트폰)가 없을 경우 결제 승인이 이루어지지 않는다. 또한 기존 결제 이미지를 재사용하고자 할 때 매번 변경되는 캡차 문자열과 이미지가 생성되어 기존의 결제 이미지와 거래 내용의 재사용은 불가하다.

4.2.3. 거래정보 습득을 통한 온라인 결제 수행

악의적인 자는 이용자의 거래정보를 탈취하기 위해 다양한 해킹 기법을 발전시켜왔고 이러한 기술은 스마트폰에서도 계속해서 진행되고 있다. 본 논문에서는 이용자의 거래정보를 보호하는 기술을 위해 보안 솔루션이 제공되는 것이 아니라 이용자 거래정보가 유출된다 할지라도 정상적인 이용자와 분리된 결제 매체를 매핑시킴으로서 본인 이외에 사용을 제한하는 방식이다. 따라서 제안한 보안기술이 온라인 결제 시스템에 적용되어 습득된 이용자 정보를 이용한 악의적인 결제가 정상적으로 수행되지 않게 된다.

Ⅴ. 설계시 고려사항

본 논문에서 제안한 전자 결제 시스템을 설계할 때 고려해야 할 운영사항에 대해서 살펴본다.

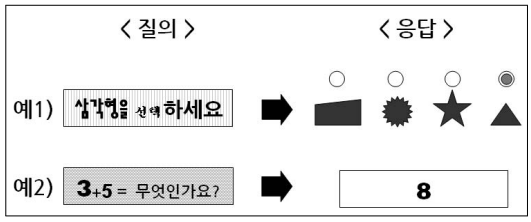
5.1. 스마트폰 결제서비스 등록 절차 검증

스마트폰 결제서비스 최초 등록 시 스마트폰 단말기의 기기정보와 추가적인 사용자 비밀번호 그리고 핸드폰 번호를 등록 받도록 해야 한다. 만일 사용자의 스마트폰 단말기 또는 폰번호가 변경되었을 경우, 기존에 등록되어진 스마트폰 단말기 기기정보, 추가 입력받은 비밀번호, 폰번호를 입력받도록 하여 기존 사용자임을 검증하는 절차가 필요하며, 또한 악의적인 사용자가 스마트폰 결제서비스의 무단 등록을 방지하기 위해 결제 서비스 등록 시 등록한 폰번호를 이동통신사로 요청하여, 적법한 사용자 여부를 검증하는 검증 절차가 필요하다. 이러한 검증 절차는 악의적인 사용자가 타 사용자의 스마트폰 결제서비스의 무단 등록을 예방할 수 있는 효과가 있으며, 이러한 효과를 높이기 위해 최초 등록된 스마트폰 단말기의 정보는 어떠한 페이지 또는 어플리케이션에서 평문으로 표현되지 않도록 해야 한다.

5.2. 신청 이미지 생성 및 관리

신청 이미지 생성 시 인증에 필요한 캡차 이미지의 경우 문자열 표현 정도에 따라 OCR(Optical Character Recognition) 기법에 의해 자동 추출될 수 있으므로 생

성될 문자열의 표현, 기울어짐, 복잡도 등의 정량화된 기준이 필요하다. 그 이유는 단순한 이미지 배경에 단순한 표현의 문자열을 캡차 이미지로 생성할 경우, 캡차 이미지내의 문자열에 대한 이용자의 인지력은 높아지나 보안성이 상대적으로 낮아지며, 반대로 복잡한 이미지 배경과 복잡한 표현의 문자열을 캡차 이미지로 생성할 경우, 보안성은 높아지나 이용자의 인지력이 낮아 인증에 방해가 되기 때문이다. 이에 대한 추가 인증 제안으로 캡차 기술과 질의응답 시스템을 이용한 인증 방식도 이를 해결하기 위한 대안이 될 수 있다.

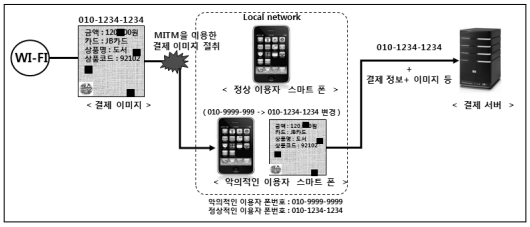


〔그림 16〕 캡차 이미지 생성방법

5.3. 안전한 네트워크 전송

이용자와 악의적인 자가 동일 네트워크 그룹에 존재하고 이용자의 거래 정보를 탈취했다고 가정할 때 악의적인 자는 탈취한 이용자의 ID/PW로 온라인 쇼핑몰에 로그인 한 후 결제를 요청한다. 이 후 서버는 신청 이미지와 결제 이미지를 전송하게 되는데 결제 이미지는 이용자가 등록한 폰번호로 전송된다. 이 때 동일 네트워크 그룹에 속해 있는 악의적인 자는 이용자에게 전송되는 결제 이미지를 도중에 가로채어 자신의 스마트폰으로 가져올 수 있다. 악의적인 자는 탈취한 이용자 거래 정보를 이용하여 상품에 대한 대금을 결제할 수 있다. 이와 같은 보안 위협을 해결하기 위해 스마트폰은 최종 결제 버튼을 전송할 때만이라도 3G 네트워크를 이용하여 결제 방식을 되도록 설계해야 한다.

〔그림 17〕 정상적인 거래절차



〔그림 18〕 결제이미지 절취를 통한 부정 결제 거래

Ⅵ. 결론

현재 전자상거래에서 발생되는 보안위협을 살펴보고 발생된 보안위협을 최소화하기 위해 본 논문에서는 결제를 위해 매체를 분리함으로써 이용자의 거래정보가 유출된다 할지라도 제안한 온라인 결제 시스템 하에서는 악의적인 자가 결제를 하기 위해 단순한 거래 정보만을 알고 정상적인 결제를 수행할 수 없다. 즉 기존의 방식은 임의 선정된 하나의 매체에서 모든 금융거래 정보를 입력하고 이를 통한 금융 거래가 이루어지도록 설계되어져 악의적인 자가 하나의 매체를 목표로 불특정 다수의 정보를 취득하고 이를 악용하였으나, 본 논문에서 제안하는 방법은 신청 매체와 결제 매체로 분리하여 악의적인 자가 얻고자 하는 정보를 2개의 매체로 분류, 소프트웨어 측면과 물리적 보안 요소측면까지 함께 고려하여 보안위협을 최소화하였다.

또한 현재의 제한적인 환경에서 제한적인 보안 기능을 제공하는 방식의 경우 급변하는 IT 환경에서 다양한 환경에서 동일한 보안성, 향상된 보안성, 신속한 보안성을 유지하기 위해서는 특정 환경에 국한되지 않은 보안 연구와 기획력이 필요한데, 본 논문에서 제안한 기술은 인터넷 환경에서 가장 기본이 되고 가장 널리 사용되고 있는 범용 이미지 표준을 이용한 결제 시스템을 구성했기 때문에 다양한 환경에서 적용 가능한 형태로 그 활용도가 높을 것으로 예상된다.

참고문헌

[1] 강신범 · 정현철. “인터넷 뱅킹 해킹 유형과 대응 기술.” *정보보호학회지*, 15권 제5호, pp. 28-37. 2005.

[2] 강전일 · 맹영재 · 김군순 · 양대헌 · 이경희. “복수의 이미지를 합성하여 사용하는 이미지 기반의 캡차와 이를 위한 안전한 운용 방법,” *정보보호학회*논

문지, 18권 제4호, pp. 153-166. 2008.
[3] 김기영 · 강동호. “개방형 모바일 환경에서 스마트폰 보안기술," *정보보호학회지*, 19권 제5호, pp. 21-28. 2009.
[4] 김성호 · 양대헌 · 이경희. “색상 정보를 이용한 문자 기반 CAPTCHA의 무력화,” *정보보호학회논문지*, 19권 제6호, pp. 105-112. 2009.
[5] 김주용 · 조인석 · 이병관. “웹사이트에서 피싱과 사기를 차단을 위한 인증기법," *한국인터넷정보학회*, 8권 제2호, pp. 137-142. 2007.
[6] 배광진 · 임강빈. “키보드 보안의 근본적인 취약점 분석,” *정보보호학회논문지*, 18권 제3호, pp. 89-95. 2008.
[7] 이정호. “전자금융 침해사고 예방 및 대응 강화 방안,” *정보보호학회지*, 18권 제5호, pp. 1-20. 2008.
[8] 정태영 · 임강빈. “키보드컨트롤러의 하드웨어 취약점에 대한 대응 방안,” *정보보호학회논문지*, 18권 제4호, pp. 187-194. 2008.
[9] 장항배 · 유일선 · 안효범. “사용자 입력정보 보호를 위한 End to End 기술연구”, *한국통신학회논문지*, 32권 제12호, pp. 377-387. 2007.
[10] 최승현 · 김강석 · 설희경 · 양대욱 · 이동욱. “스마트폰 전자금융거래 보호를 위한 법제적 문제점 분석 - 전자금융거래법(안)을 중심으로 -”, *정보보호학회논문지*, 20권 제6호, pp. 67-81. 2010.
[11] 이철 · 김용만 · 유승재. “스테가노그라피를 활용한 정보은닉 응용기법 연구”, *한국사이버테러정보전학회*, 10권 제2호, pp. 19-26. 2010.

〈著者紹介〉

진 승 만 (Jin Seung man)
2002년 2월 : 전북대학교 컴퓨터공학과 졸업
2006년 8월 : 연세대학교 컴퓨터공학과 석사
2011년 10월~현재 : 전북은행 정보보호팀 과장
<관심분야> 금융보안, 전자금융거래 및 인증, 전자상거래, IT컴플라이언스