情 報 保 護 學 會 誌
第23卷 第1號, 2013. 2

다중채널 기반의 안전한 금융거래 입력방식

박 영 록*, 손 진 우**, 신 선 호***, 윤 명 근****

요 약

인터넷과 스마트폰을 이용하는 전자금융거래가 보편화됨에 따라 안전한 거래를 위한 보안 기술이 중요해지고 있다. 현재 많은 보안 솔루션들이 사용되고 있으나, PC만을 이용한 거래 혹은 스마트폰만 이용하는 거래는 공격자에게 단말기가 해킹당한 경우, 사용자가 단말기에 입력하는 정보가 공격자에게 유출될 수 있는 문제점이 존재한다. 이러한 정보 유출 문제를 해결하기 위해서 우리는 다중 채널을 이용하여 입력과 출력을 분리하는 새로운 접근 방법을 제안하고, 안드로이드 스마트폰과 윈도우즈 기반의 PC에 직접 구현하여 인터넷뱅킹 시나리오에 적용하여 실효성을 검증한다. 제안하는 방식은 전자금융거래 뿐만 아니라 사용자 입력이 필요한 모든 입력방식의 안전성을 높이는데 활용될 수 있다.

Ⅰ. 서 론

2012년 1/4분기 말 현재 인터넷뱅킹 서비스 등록 고객 수는 8,015만 명으로 이전 분기 대비 7.1% 증가하였다. 인터넷뱅킹서비스 이용건수는 일평균 4,523만 건으로 전 분기대비 9.5% 증가하였으며, 이용금액은 33조 1,814억 원으로 0.5% 증가하였다 [1]. 모바일 뱅킹(Mobile Banking) 서비스 등록 고객 수는 전 분기 말(2,372만 명) 대비 339만 명(+14.3%) 증가한 2,711만 명으로 추산된다. 이 중 스마트폰 기반 모바일뱅킹 등록 고객 수는 전분기말에 비해 331만 명(+31.9%) 증가한 1,367만 명에 달한다 [1]. [표 1]은 모바일 뱅킹 서비스 이용 실적을 보여준다.

고객수와 이용건수가 늘어남에 따라 전자금융거래에 대한 정보보호가 큰 이슈가 되고 있다. 현재 인터넷뱅킹에서 사용되는 보안 솔루션으로는 공인인증서, 일회용 비밀번호(OTP: One Time Password), 보안카드, 가상키보드 등이 있다. 사용자인증과 전자서명, 그리고 암호화를 위해서 공인인증서가 사용되고 있으며, 재전송공을 막기 위해서 일회용 비밀번호와 보안카드가 사용되고 있다. 또한, 공격자에 의한 사용자 PC 장악과 정보유출을 막기 위해서 키보드보안 솔루션이 사용되고 있다.

〔표 1〕 모바일 뱅킹 서비스 이용 실적(일평균) [2]

〈단위 : 천건, 십억원, (모바일뱅킹 비중, %)〉

구분	2009년	2010년	2011년
전체 이용건수	1,721(6.5)	3,736(11.2)	7,697(19.7)
스마트폰	19	907	5,910
전체 이용금액	266.2(1.0)	415.6(1.4)	625.6(2.0)
스마트폰	0.0	46.7	372.7

하지만 기존 보안솔루션들은 PC 또는 스마트폰 단일 채널에서만 작동하기 때문에 공격자가 해당 채널을 장악하는 경우, 사용자가 입력한 모든 정보가 공격자에게 유출되는 문제점을 근본적으로 가지고 있다. 예를 들어,

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2010-0008708 & 2011-0016246).
* 국민대학교 전자정보통신대학 컴퓨터공학부 정보보호연구실 (Adamas@kookmin.ac.kr)
** 국민대학교 전자정보통신대학 컴퓨터공학부 정보보호연구실 (jinwooson@kookmin.ac.kr)
*** 국민대학교 전자정보통신대학 컴퓨터공학부 정보보호연구실 (shshin@kookmin.ac.kr)
**** 국민대학교 전자정보통신대학 컴퓨터공학부 정보보호연구실 (mkyoon@kookmin.ac.kr)

사용자PC가 공격자에 의해 장악 당한 상태라면, 공격자는 키로거(key logger)나 화면전송 등의 기술을 이용해서 사용자가 입력하는 정보(계좌정보, 통장비밀번호, 로그인 ID/PWD, 이체비밀번호 등)를 알아낼 수 있다. 기존의 일회용 비밀번호와 보안카드를 사용하면 재전송공격을 어느 정도 막을 수 있지만, 정보유출 자체를 차단하지는 못한다. 사용자의 계좌번호, 이체내용, 통장비밀번호 등의 정보는 여전히 유출될 가능성이 존재한다. 실제로 2011년 9월 20일 행정 안전부 국정감사장에서 해킹시연을 통해서 개인의 PC가 공격자에 의해 장악되는 경우 주요 정보가 유출된다는 것이 증명된 바 있다. 사용자가 PC대신 모바일뱅킹 서비스를 이용한다고 하여도 동일한 위험은 존재한다 [3].

우리는 이러한 사용자 입력정보의 유출문제를 해결하기 위해서 멀티채널 기반의 일회용 가상 키패드 입력 시스템을 제안한다. 제안하는 방식은 둘 이상의 통신채널과 사용자단말을 이용하여 키패드 출력과 입력을 분산시킨다. 키패드는 세션별로 매번 다르게 일회용으로 생성되기 때문에 높은 보안성을 제공한다. 제안하는 방식은 멀티채널과 키패드가 모두 공격자에게 장악되지 않는 이상, 사용자가 입력하는 정보가 공격자에게 유출되지 않는 안전성을 제공한다. 본 논문에서는 편의상 인터넷 기반 PC채널(이하 인터넷채널)과 3G망 기반 스마트폰채널(LTE채널 포함, 이하 3G채널로 통일하여 지칭함)로 구성된 이중채널의 사용을 가정한다. 하지만 적용환경에 따라서 단말과 채널의 개수를 증가시키거나 종류를 변경시킬 수 있다. 기본 모드를 인터넷채널과 3G채널로 설정한 이유는 스마트폰과 휴대폰이 일반화되었기 때문이며 인터넷에 접속된 PC를 손쉽게 접근할 수 있기 때문이다.

Ⅱ. 관련 연구 및 동향

인터넷뱅킹의 정보보호 솔루션을 인증기술, 키보드 보안기술, 멀티채널기술로 분류하여 설명한다.

2.1. 인증기술

인터넷뱅킹의 인증팩터를 분류해 보면 [표 2]과 같이 나눌 수 있다. 여기서는 공인인증서, 보안카드, 일회용 비밀번호에 대해서 살펴본다. 키보드보안과 멀티채널은 다음 챕터에서 별도로 다루도록 한다.

〔표 2〕 인증팩터 분류 [4, 5]

분 류	예 시
지식 기반	아이디/비밀번호, 공인인증서 비밀번호, 계좌 비밀번호, ISP 비밀번호 등
소지 기반	일회용비밀번호(OTP) 발생기, HSM, 보안카드, 스마트카드 등
특징 기반	지문, 홍채, 정맥 등

2.1.1 공인인증서

공인인증서는 PKI(Public Key Infrastructure)를 구현하는데 필요한 핵심 기술로서 사용자가 개인키를 소지하고 있다가 필요한 순간에 사용하는 소지기반 기술이다. 전자금융거래에서 보면 공인인증서는 크게 두 가지 역할을 한다.

첫째, 사용자는 거래내용에 대해서 개인키로 전자서명을 하여 거래에 대한 본인의 의사를 전자문서로 남긴다. 서명자의 개인키는 서명자만이 알고 있기 때문에 부인봉쇄 서비스가 제공된다. 부인봉쇄는 다른 보안기술들로는 보장해주기 어렵기 때문에 공인인증서만의 특징이라고 볼 수 있다. 개인키로 서명된 내용을 확인하여 사용자 인증 용도로도 사용하는데, 로그인 기능이 좋은 사례이다. 즉, 인터넷 뱅킹 서버에는 고객의 각종 정보들이 저장되어 있는데, ID, 주소, 계좌번호 등이 고객의 프로파일(profile)을 구성하고 있다고 가정하자. 이 프로파일에 고객의 인증서를 추가하여 고객이 인증서를 이용해서 로그인하려고 하면, 서버는 특정 메시지를 고객에게 제시하고 고객은 해당 메시지를 개인키로 서명하여 서버에 제출한다. 서버는 서명 값을 검증함으로써 고객을 인증하게 된다.

둘째, 상대방의 공개키를 사용해서 전송하는 메시지의 기밀성을 제공한다. 상대방의 공개키로 암호화된 내용은 그 키에 해당하는 개인키로만 복호화 되기 때문에 전송되는 메시지를 개인키 소유자 이외의 사람은 알아내지 못한다.

공인인증서 비밀번호의 경우 사용자가 발급 받을 때 직접 설정하기 때문에 Brute-Force 공격 또는 사전 공격(Dictionary Attack)으로 노출 될 위험을 가지고 있다. 이러한 방식의 공격으로 공격자가 인증서의 비밀번호를 획득할 경우 손쉽게 사용자의 권한을 얻어 인터넷 뱅킹 서비스에 접근이 가능하게 된다. 공인인증서의 또

다른 약점은 갱신 및 재발급 정책이다. 공인인증서는 1년이 지날 경우 갱신 혹은 재발급을 받아야 한다. 만일 공격자가 갱신 혹은 재발급 시 사용자 PC를 장악한다면 키로거 등 악성 프로그램 등을 이용하여 공인 인증서의 비밀번호를 탈취할 수 있다.

2.1.2 보안카드

보안카드는 소지기반의 인증요소이다. 금융기관에서는 약 35개의 난수로 구성된 보안카드를 고객에게 나누어 준다. 사용자는 전자금융거래 시 서버가 요청하는 번호를 보안카드에서 찾아서 입력하고 서버는 입력한 번호와 요청한 번호의 일치여부를 판단하여 거래를 진행한다.

보안카드의 경우 소지기반의 비밀번호이고 금융기관마다 독립적으로 발급한다. 그리고 보안카드의 수들은 난수이지만 35개 이내의 고정된 수이다. 사용자의 보안카드는 소지기반이기 때문에 여러 금융기관 거래 시 많은 수의 보안카드를 소지하여야 하는 불편함을 갖는다. 이러한 불편함 때문에 스캔하여 보관하거나 사용자 PC에 저장하거나, 복사하여 문서상으로 보관하는 경우가 발생한다. 스캔하여 보관할 경우 공격자에게 사용자의 PC가 장악된다면 보안카드의 비밀번호가 쉽게 노출 된다는 단점을 가지고 있고, 복사하여 보관 할 경우 하나의 일련번호에 하나만 존재해야 할 보안카드의 목적에서 벗어나게 된다. 그리고 소지기반으로 인한 문제뿐만 아니라 35개 이내의 고정된 난수로 구성되어 있기 때문에 공격자가 지속적인 모니터링을 통하여 보안카드의 비밀번호를 알아낼 가능성이 존재한다.

2.1.3 일회용 비밀번호(One-Time Password)

동일한 비밀번호를 사용할 경우 비밀번호의 노출과 그로 인한 재전송 공격이 가능해진다. 이러한 문제점을 해결하기 위해서 일회용 비밀번호 생성기를 이용하여 로그인 세션마다 매번 다른 난수를 생성하며 매번 새로운 비밀번호를 입력하여 사용할 수 있다. 일회용 비밀번호 인증 방식은 질의응답방식, 이벤트 동기화 방식, 시간동기화 방식 등이 있다 [6, 7]. 일회용 비밀번호는 매번 새로운 비밀번호를 생성하여 공격자가 비밀번호를 수집한다고 하여도 재사용공격이 불가능해진다.

[그림 1]은 일회용 비밀번호의 동작원리를 보여준다. 일회용 비밀번호 생성기를 통하여 비밀번호를 생성하고 생성된 비밀번호는 금융기관에 전송된다. 금융기관에서도 일회용 비밀번호를 생성하여 생성된 값과 사용자로부터 입력받은 값이 일치하는지 검증한다. 일치할 경우에만 사용자 인증이 성공한다. 일회용 비밀번호는 사용자의 로그인 세션정보 또는 시간정보를 이용하여 생성되는 난수이다. 일반적으로 사용자가 직접 설정하는 비밀번호는 의미를 갖는 비밀번호일 가능성이 높다. 하지만 일회용 비밀번호의 경우 의미가 없는 숫자로 구성되며 패턴 또한 보이지 않고 비밀번호의 유효시간 또한 매우 짧게만 존재한다. 하지만 이러한 일회용 비밀번호도 한계점은 있다. 일회용 비밀번호를 사용하기 위해서는 일회용 비밀번호 생성기를 소지하고 있어야 한다. 실시간 피싱(Phishing) 또는 MITM(man-in-the-middle) 공격에 대해서도 약점을 가지고 있다. 즉, 사용자가 일회용 비밀번호를 통하여 인증을 시도할 경우 공격자는 중간에서 일회용 비밀번호의 정보를 가로채 거래를 정상적으로 수행하지 못하도록 할 수 있다.

〔그림 1〕 일회용 비밀번호 생성기 동작 원리 [6]

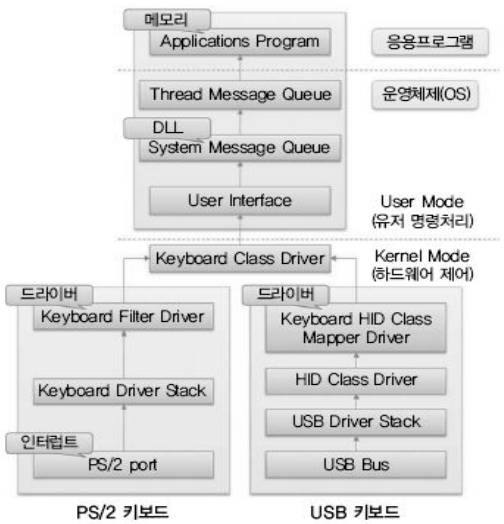
2.2 키보드보안 프로그램

키보드보안 프로그램은 사용자의 PC가 공격자에게 점령당하여 키로거 같은 악성 프로그램으로부터 중요정보가 노출 되는 것을 막기 위해서 사용된다. [그림 2]는 키가 입력 된 뒤 데이터가 전송되는 흐름을 보여주고 있으며, 입력 값을 탈취할 수 있는 구간이 많이 존재함을 알려준다.

국내 키보드 보안 프로그램들은 키 값 탈취가 가능한 구간의 입력 값들을 각자의 방식으로 암호화하여 데이터를 보호한다. 그리고 키로거가 입력 값을 가로채지 못

하도록 더미(Dummy)값을 상위단계로 올려 보내도록 되어있다. 이러한 방식으로 키보드 보안 프로그램은 사용자가 입력하는 중요한 정보를 암호화하여 정보 노출을 방지한다[8].

키보드 보안 프로그램에도 문제점은 존재한다. 사용자가 정상적인 설치를 하지 않거나 동작하지 않을 경우가 있다. 이런 경우 기능이 최소화 된 키보드 보안 프로그램을 제공하지만, 해당 프로그램들은 후킹 위험에 노출 되어있다 [8]. 만약 공격자가 사용자가 인지하지 못하게 기능이 최소화 된 키보드 보안프로그램을 설치하거나 아예 설치하지 못하게 한다면 공격자는 사용자의 정보를 획득 할 수 있다.



〔그림 2〕 키 입력 전송 흐름 [8]

2.3 멀티채널(Multi Channel)

멀티채널 방식은 인터넷 이외의 별도로 통신 채널을 이용하여 거래의 안전성을 높여준다. 일반적으로 메인 채널은 PC 인터넷을 사용하고, 사이드 채널은 핸드폰 무선통신망을 이용한다. 멀티채널 인증 방식일 경우 메인채널이 공격자에게 장악당해도 사이드 채널이 장악당하지 않으면 안전하다. 현재 사용되고 있는 멀티채널의 한 사례는 전화승인 서비스이다. 고객은 은행 서버에 본인의 핸드폰 연락처를 등록한다. 연락처를 등록한 고객이 PC를 사용해서 공인인증서와 보안카드, 혹은 일회용 비밀번호를 이용하여 거래를 진행한다. 이 때 은행에서는 자동응답 시스템을 통하여 고객에게 현재 거래하려는 내용을 음성으로 알려준다. 고객은 이 음성의 내용을 통하여 거래 진행 내역을 한 번 더 확인하고 정상 진행 또는 취소 선택이 가능하다 [7].

기존 멀티채널은 두 가지 문제점을 가지고 있다. 첫째, 사용자가 두 번째 채널을 통해서 거래 내역을 잘 확인한 후에 거래를 진행해야 한다. 그렇지 않으면 공격이 성공할 수 있다. 둘째, PC와 인터넷 채널을 통해서 공격자는 사용자가 입력하는 내용(계좌정보, 이체 비밀번호 등)을 여전히 수집할 수 있다. 우리는 이번 논문을 통해서 두 번째 문제를 해결할 수 있는 방법을 제안한다.

Ⅲ. 멀티채널을 이용한 일회용 가상 키패드설계

본 장에서는 기존 보안 솔루션들로는 해결하지 못하는 사용자 입력 정보 유출 문제에 대해서 상세히 기술하고, 이 문제를 해결할 수 있는 멀티채널 기반의 일회용 가상 키패드를 제안한다.

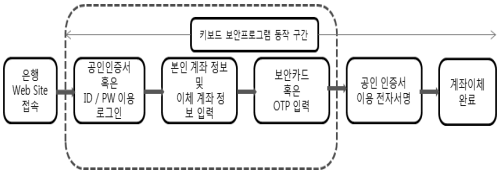
3.1 문제 정의

전자금융거래를 성립시키기 위해서는 사용자가 단말기에 정보를 입력해야 한다. 가령, PC를 이용한 인터넷 뱅킹 사례에서는 사용자가 계좌정보, ID/PWD, 통장 비밀번호 등을 PC 입출력 장치(I/O device)-주로 키보드나 마우스 클릭-를 통해서 입력한다. 이때, 공격자가 PC를 완벽하게 장악한 상태라면 어떤 값이 입력되는지를 알아 낼 수 있다. 이 문제는 OTP를 이용하더라도 근본적으로 해결될 수 없다. 현재 OTP는 강력한 사용자 인증을 위해서 사용되고 있는데, 사용자가 출금이체 계좌번호를 입력하거나 외우고 있는 통장 비밀번호를 입력하는 경우에는 별다른 도움이 되지 못한다. 특히, 생성된 OTP 숫자도 사용자가 PC에 입력하는 순간에 공격자에게 일차적으로 노출이 되는 것을 막을 수는 없다.

우리는 이번 연구를 통해서 사용자가 입력하는 어떠한 정보도 공격자에게 유출되지 못하게 하는 가상 키패드 기술을 제안한다. 제안하는 방식에서는 멀티채널을 이용해서 한 쪽 채널로는 일회용 키패드 배열을 사용자에게 “*출력*”해 주고, 다른 채널로는 사용자로부터 값을 “*입력*” 받아 서버로 전송해줌으로써 사용자 입력 정보가 공격자에게 유출되지 않도록 한다. 단, 멀티채널 중

적어도 한 채널은 동일한 공격자에게 장악되지 않았다는 가정 하에 안전성이 보장된다. 이러한 가정은 기존의 멀티채널 방식에서 받아들여져 왔으며, 필요에 따라서 멀티채널의 종류와 수를 늘림으로써 보안성을 더욱 높일 수 있다.

제안하는 멀티채널을 이용한 일회용 가상 키패드 기술은 전자금융거래는 물론이고 모든 범용 전자장비의 입력방식에 적용이 가능하다. 이번 논문에서는 편의상 인터넷뱅킹 계좌이체 서비스를 대상으로 제안하는 방식을 설명하도록 한다.

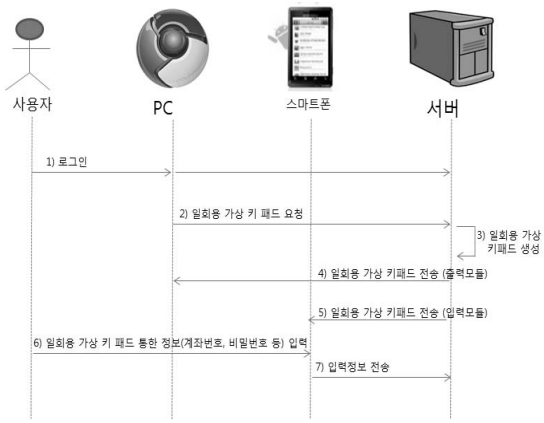


〔그림 3〕 계좌이체 서비스 흐름도

[그림 3]은 인터넷 뱅킹 계좌이체 서비스의 진행 과정을 보여준다. 사용자는 금융기관 홈페이지에 접속 후 공인 인증서 혹은 등록 되어 있는 ID/비밀번호를 이용하여 로그인을 한다. 로그인을 완료한 뒤 계좌이체 서비스 이용을 위해 필요한 정보를 입력한다. 서비스를 정상적으로 완료하기 위하여 금융기관 서버는 보안카드 혹은 일회용 비밀번호를 통해 사용자 인증을 요구한다. 사용자 인증이 정상적으로 수행 될 경우 마지막으로 공인인증서를 이용하여 전자서명을 한 뒤 계좌이체를 정상적으로 완료된다. [그림 3]의 붉은 색으로 표시된 부분이 사용자를 인증하는 구간이다. 사용자를 인증하는 방법으로는 ID/PWD, 공인인증서, 일회용비밀번호, 보안카드 등이 있다. 그리고 입력 값들을 보호하기 위한 솔루션으로 키보드 보안 프로그램이 동작하고 있다. 하지만 앞 절에서 설명하였듯이 현재 처리과정이 단일채널에서 동작하고 있기 때문에 해당 채널이 공격자에게 장악당할 경우 사용자 입력정보가 쉽게 공격자에게 노출된다. 우리는 이러한 문제점을 해결하기 위해서 멀티채널 기반의 가상 키패드 시스템을 제안한다.

3.2 멀티채널을 이용한 일회용 가상 키패드 시스템

[그림 4]는 본 논문에서 제안하는 멀티채널을 이용한 일회용 가상 키패드 시스템의 구성도와 실행 순서를 나타낸다. 사용자는 인터넷뱅킹 서비스 중 계좌이체 서비스를 이용하려고 한다. 사용자는 인터넷 채널을 갖춘 PC와 3G 채널을 갖춘 스마트폰으로 구성된 이중채널을 이용한다. 서버는 인터넷뱅킹 서버를 나타낸다. 실행 순서를 세부적으로 설명하면 다음과 같다.



〔그림 4〕 멀티채널을 이용한 가상 키패드 구성

1) 사용자 로그인 인증 과정을 나타낸다. 공인인증서, OTP, ID/PWD 등 다양한 인증 방법이 사용 가능하다. 이 과정에서는 일회용 가상 키패드를 사용하지 않는다.

2) 사용자 입력이 필요한 시점에 PC는 서버에 일회용 가상 키패드의 생성 및 배포를 요청한다.

3) 서버는 사용자 로그인 세션 정보와 서버에 저장된 비밀정보, 시간정보를 이용해서 일회용 가상 키패드를 생성한다. 가상 키패드는 출력모듈과 입력모듈로 구성된다. 각 모듈에 대한 자세한 내용은 다음 장에서 설명한다.

4) 서버는 일회용 가상 키패드 중 출력모듈을 PC로 전송한다. PC 스크린에 일회용 가상 키패드 화면이 표시된다 ([그림 5] 참조).

〔그림 5〕 일회용 가상 키패드 출력모듈 (PC화면)

5) 서버는 일회용 가상 키패드 중 입력모듈을 스마트

〔그림 6〕 일회용 가상 키패드 입력모듈 (스마트폰 화면. 자판별 4자리 숫자는 사용자에게 보이지 않음)

폰으로 전송한다. 스마트폰의 전화번호는 사전에 등록되어 있었다고 가정한다. 입력모듈은 키패드에 문자나 숫자가 보이지 않으며, 오직 자판 배열만이 표시된다([그림 6] 참조).

6) 사용자는 PC 화면과 스마트폰 화면을 동시에 보면서 PC 화면 키패드 위치에 해당하는 숫자를 스마트폰 입력모듈 키패드를 터치하여 입력한다. 예) “1234”를 입력해야 하는 경우라면 PC화면([그림 5])을 보면서 스마트폰화면([그림 6])의 “CBE9-B6E5- 23C2-D8E5”를 순서대로 클릭한다.

7) 입력된 정보가 서버로 전송되어 검증된다. 서버는 출력모듈과 입력모듈간 자판 배열의 매핑정보를 가지고 있기 때문에 입력된 숫자의 원래 의미를 복원할 수 있다.

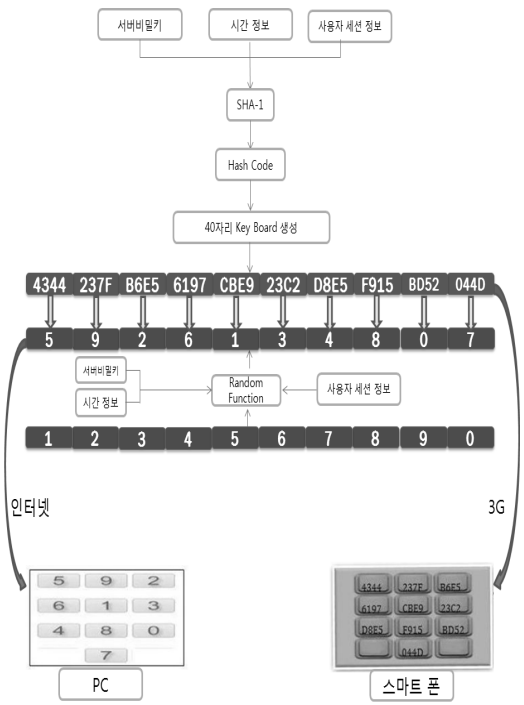
3.2.1 일회용 가상 키패드 생성 메커니즘

서버는 사용자가 가상 키패드를 요청할 경우 서버의 비밀정보(K: 서버만 아는 비밀키 값)와 세션정보(SID), 시간 정보(T)를 이용하여 가상 키패드를 생성한다.

[그림 7]은 가상 키패드가 생성되는 과정을 보여준다. 사용자가 가상 키패드를 요청하면 서버에서 가상 키패드를 생성하여 입력모듈을 3G망을 통해서 스마트 폰으로 전송하고 스마트 폰에서는 입력할 수 있는 더미패드(dummy)를 생성한다. 더미패드에는 숫자가 적혀져 있지 않다. 반면 출력모듈은 인터넷을 통해서 서버에서 PC로 전송된다.

[그림 7]에서와 같이, PC로 전송되는 출력모듈에는 10개의 숫자가 임의로 배열된다 (“5-9-2-6-1-3-4-8-0-7”). 배열 규칙은 서버 비밀키, 시간정보, 사용자 세션정보를 조합해서 랜덤함수를 이용해서 생성한다. 비슷한 방식으로 스마트폰 쪽으로 전송되는 더미패드도 생성된다. 더미패드 역시 10개의 숫자로 구성되는데, 실제 사용자 화면에는 아무것도 쓰여 있지 않은 키자판 10개만이 보여 진다. 하지만 각 자판은 내부적으로 4자리 숫자와 매핑 되어 있는데, 이 매핑을 생성하기 위해서 SHA-1에 서버 비밀키, 시간정보, 사용자 세션정보를 입력하여 난수를 생성시키고 40자리 키보드를 생성한다([그림 7]의 파란색 바탕 흰색 10개의 숫자 부분). 서버는 출력모듈로 전송될 10개의 자판과 입력모듈로 전송될 10개의 자판 사이의 매핑관계를 기억한다.

사용자가 PC화면과 스마트폰화면을 이용해서 비밀번호, 계좌정보 등의 값을 입력하면 해당 정보는 스마트폰에서 암호화되어 3G채널로 전송된다. 즉, 사용자가 스마트폰 어플리케이션을 통해 비밀번호를 입력하면 실제 비밀번호가 전송되는 것이 아니라 각 자리에 매핑된 문자열이 전송되고. 서버는 앞의 과정에서 생성한 출력모듈과 입력모듈간 키패드 매핑관계를 이용해서 사용자가 입력한 정보를 원래 숫자대로 복원한다. 예) “CBE9-B6E5- 23C2-D8E5”를 “1234”로 복원함. 전송되는 정보의 무결성을 높이기 위해서 HMAC(Hash-based Message Authentication Code)을 사용한다.



〔그림 7〕 가상 키패드 생성 프로세스

3.2.2 정보유출 안전성

이중채널을 이용한 일회용 가상 키패드는 어느 한 채널이 공격자에게 장악되더라도 사용자가 입력한 정보가 공격자에게 유출되는 것을 막을 수 있다. PC와 스마트폰이 각각 공격자에게 장악당한 상황에서 정보유출이 차단되는 과정을 보이면 다음과 같다.

첫 번째 시나리오로서 인터넷-PC가 공격자에게 장악되었다고 가정하자. 공격자는 일회용 가상 키패드를 포함한 모든 PC화면을 볼 수 있다. 하지만 사용자는 스마트폰에 정보를 입력하고 3G망을 통해서 서버에 전송되기 때문에 어떤 숫자가 입력되었는지 알 수 없다.

두 번째 시나리오로서 3G-스마트폰이 공격자에게 장악되었다고 가정하자. 공격자는 사용자가 선택한 키패드의 위치와 입력 순서를 알아낼 수 있다. 하지만 선택된 자판이 의미하는 숫자를 알 수 없기 때문에 입력된 정보를 유출할 수 없다.

3.2.3 멀티채널 확장성

이중채널을 사용하는 환경에서는 만약 두 채널이 공격자에게 동시에 장악되었다면 공격자는 입력모듈과 출력모듈을 모두 관찰함으로써 사용자가 입력하는 정보를 알아낼 수 있다. 일반적으로 두 채널이 동일한 공격자에게 동시에 장악되는 경우는 매우 드물게 발생한다고 여겨진다. 실제로 기존의 전자금융거래의 보안대책을 수립할 때에도 이중채널이 사용되면 보안성이 크게 향상된다고 가정하고 있다. 그럼에도 불구하고 이중채널을 삼중, 사중으로 확장하면 그만큼 공격자에 의한 정보유출이 차단될 가능성이 더욱 높아진다. 공격자는 모든 채널을 장악해야지만 사용자가 입력한 내용을 확인할 수 있기 때문이다. 예를 들어, 하나의 채널이 공격자에게 장악될 확률을 p라고 하자. n개의 멀티채널이 사용되고 있는 상황이라면, 공격자가 사용자 입력정보를 알아낼 확률 q는 $q=p^n$를 만족한다. 일반적으로 p 값이 크지 않기 때문에 q는 n이 증가할수록 큰 폭으로 감소된다. 예를 들어 p가 10^{-3}이라면 이중채널을 사용하는 경우 입력정보가 유출될 확률은 10^{-6}가 되고, 삼중채널을 사용하게 되면 확률은 10^{-9}로 줄어들게 된다.

이중채널을 삼중 이상의 멀티채널로 확장하기 위한 구현 방법으로서 입력모듈을 확장하는 방식과 출력모듈을 확장하는 방식을 고려해 볼 수 있다. 하지만 입력모듈이 많아지면 그만큼 입력을 여러 단말기에서 나누어 해야 하기 때문에 사용 편이성이 크게 떨어진다. 반면에 출력모듈을 확장하면 이러한 문제를 해결할 수 있다. [그림 8]는 출력모듈 두 개(PC, 스마트폰1)와 입력모듈 한 개(스마트폰2)로 구성된 삼중채널 일회용 가상 키패드를 보여준다. 스마트폰 두 대와 PC 한 대로 구성된 상황에서 한 대의 스마트폰이 입력모듈을 담당하고 나머지 스마트폰과 PC가 출력모듈을 구성한다. 각 출력모듈은 5개의 키패드 정보를 가지고 있다.

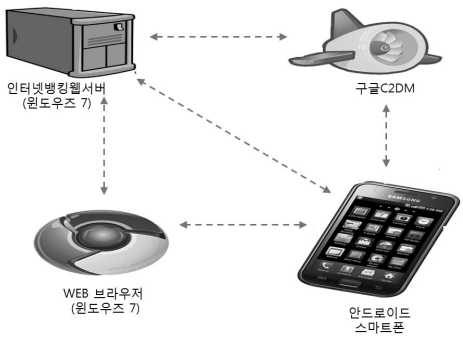
〔그림 8〕 스마트폰 2대와 PC 1대로 구성된 삼중채널 일회용 키패드

Ⅳ. 구현 및 검증

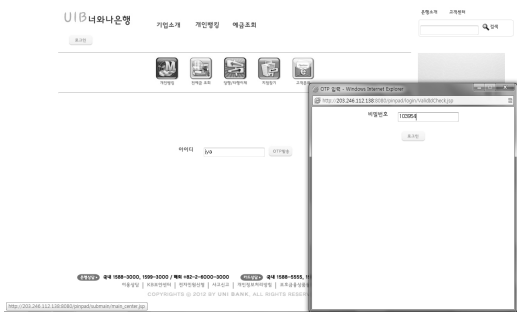
우리는 윈도우즈7 PC와 안드로이드 스마트폰을 이용해서 이중채널 기반의 일회용 가상 키패드를 구현했다. JSP(Jave Server Pages)를 사용해서 간단한 인터넷 뱅킹 홈페이지를 구축하였으며, 안드로이드 스마트폰과 웹서버의 메시지 통신을 위해서 구글에서 제공하는 C2DM(Cloud to Device Messaging)을 사용하여 서버의 푸시 메시지를 구현했다 [9]. 웹서버는 아파치 톰캣 6.0을 이용하여 구현했으며, 서버의 데이터베이스는 MYSQL를 사용하였다. 스마트 폰 어플리케이션은 안드로이드 SDK 2.3(진저브레드)를 이용하여 개발하였고 어플리케이션의 데이터베이스는 SQLite를 이용하여 구축하였다. [그림 9]는 우리가 구현한 시스템의 구성을 보여준다. 웹서버에는 일회용 가상 키패드를 생성하는 핵심모듈이 구현되어 있다. 안드로이드 스마트폰에서는 더미 키패드 화면을 출력해주고 사용자로부터 터치스크린으로 숫자를 입력받아 암호화시켜서 서버로 전송해주는 기능이 앱(App)으로 구현되었다.

[그림 10]의 웹 페이지는 가상의 인터넷뱅킹 사이트를 구현한 것이다. 사용자는 인터넷뱅킹 서비스를 이용하기 위해서 로그인이 필요하다. 우리는 일회용 비밀번호 방식을 사용해서 사용자 로그인을 구현했다. 사용자

가 아이디를 입력하고 일회용비밀번호 발송 버튼을 클릭하면, [그림 10] 오른쪽 그림과 같이 일회용비밀번호 입력창이 생성된다. 서버는 일회용 비밀번호를 생성하고 사용자의 스마트폰으로 일회용비밀번호를 전송한다. 구글의 C2DM 서버에 사용자의 장치 정보가 저장되어 있다. 서버는 구글의 C2DM서버로 일회용비밀번호를 전송하고 C2DM서버는 사용자의 장치로 일회용비밀번호를 전송한다.



〔그림 9〕 구현된 이중채널 일회용 가상 키보드 시스템 구성도



〔그림 10〕 일회용 비밀번호를 요청하는 웹페이지

[그림 11]은 사용자의 스마트폰 앱이 전송받은 일회용비밀번호를 보여준다. 사용자는 이 정보를 확인하여 [그림 11] 오른쪽 팝업창에 비밀번호를 입력한다.

[그림 12] 화면은 사용자가 계좌이체를 수행하는 화면이다. 계좌이체에 필요한 정보를 입력 한 뒤 사용자는 본인 인증에 필요한 비밀번호 입력을 위해 멀티채널 일회용 가상키보드 불러오기 버튼을 클릭한다. 버튼을 클릭하면 서버는 자체적으로 가상 키패드를 생성한다. 서버는 PC에 출력모듈을 전달하고 [그림 12], 그림의 오른쪽 화면과 같이 랜덤하게 배열된 키패드 출력모듈이

〔그림 11〕 일회용 비밀번호 전송 화면

〔그림 12〕 일회용 가상 키패드 출력모듈

제시된다. 또한 서버는 가상 키패드 입력모듈을 생성하고 구글의 C2DM서버를 이용해서 사용자의 스마트폰에 키패드 입력모듈을 전송한다.

[그림 13]은 [그림 7]의 설계를 이용하여 생성된 가상 키패드 입력모듈이다. 사용자의 스마트폰 앱이 서버로부터 키패드 입력모듈을 수신하면 앱은 비밀번호 입력을 위한 더미자판을 [그림 13]과 같이 생성한다. 사용자는 [그림 12]의 키패드 출력모듈을 보면서 비밀번호에 해당하는 더미자판의 위치를 순서대로 클릭한다. 최종

〔그림 13〕 스마트폰 앱으로 구현한 가상 키패드 입력모듈

적으로 입력이 완료되면 [그림 13]과 같이 랜덤하게 보이는 문자열(“FCDC67FSBA706EB1”)이 서버로 전송된다. 서버는 일회용 가상 키패드의 입력모듈과 출력모듈의 자판 배열 매핑 정보를 이용해서 랜덤한 문자열을 복호화 시키고 유효한 비밀번호가 맞는지 확인한다. 비밀번호가 유효할 경우 거래를 정상적으로 진행시킨다.

Ⅴ. 결론

본 논문에서는 단일채널 기반의 기존 보안솔루션으로는 막을 수 없는 사용자 입력정보 유출문제에 대해서 연구했으며, 이러한 문제를 해결할 수 있는 방법으로 멀티채널을 이용한 일회용 가상 키패드 시스템을 제안했다. 정보입력에 사용되는 키패드를 입력모듈과 출력모듈로 분류하여 멀티채널로 각각 전송시킴으로써 한 채널이 공격자에 의해서 점령당하더라도 정보유출을 방지할 수 있다. 또한 제안한 시스템을 윈도우즈 PC와 안드로이드 스마트폰에 실제 프로그램으로 구현하여 검증하였다. 제안한 일회용 가상 키패드 시스템은 전자금융거래는 물론 일반 정보기기에서도 안전한 사용자 정보 입력 범용 기술로서 사용될 수 있다.

참고문헌

[1] 한국은행, “2012년 1/4분기 국내 인터넷뱅킹서비스 이용현황”, 2012.05.18.

[2] 최한묵, “금융과 정보기술[IT]", 금융감독원, 2012.7

[3] 오병민, http://www.boannews.com/media/ view.asp?idx=27855, 보안뉴스, 2011.10.05.

[4] 맹영재, 신동오, 김성호, 양대헌, “전자금융거래에서의 문서변조 취약점 분석 및 대응방법 고찰”, *정보보호학회논문지*, 제20권 제6호, pp.17-27, 2010. 12

[5] 금융보안연구원, “전자금융 신 인증기술 연구보고서”, 금융보안연구원, 2011.3

[6] 강우진, “OTP 통합인증서비스 소개”, 금융보안연구원, 2010.12.30.

[7] H. You, J. Lee, J. Kim, M.Jun, "A study on the two-channel authentication method which provides two-way authentication in the Internet banking environment", Computer Sciences and Convergence Information Technology (ICCIT), 2010.12

[8] 맹영재, 신동오, 김성호, 양대헌, 이문규, “국내 인터넷뱅킹 계좌이체에 대한 MITB 취약점 분석”, *Internet and Information Security*, 제1권 제2호, pp.101-118, 2010.11

[9] Google, "https://developers.google.com/android/c2dm/"

〈著者紹介〉

박 영 록 (Park, YoungLok)
2013년 2월 : 국민대학교 컴퓨터공학부 학사.
2013년 3월 : 국민대학교 컴퓨터공학부 대학원 입학 예정.
<관심분야> 금융보안, 정보보호

손 진 우 (Son, JinWoo)
2013년 2월 : 국민대학교 컴퓨터공학부 학사.
2013년 3월 : 국민대학교 컴퓨터공학부 대학원 입학 예정.
<관심분야> 네트워크 알고리즘, 클라우드 컴퓨팅

신 선 호(Shin, SeonHo)
학생회원
2011년 2월 : 국민대학교 컴퓨터공학부 학사
2012년 8월 : 국민대학교 컴퓨터공학부 석사
2012년 9월 ~ 현재 : 국민대학교 컴퓨터공학부 박사과정
<관심분야> 네트워크 알고리즘 & 보안

윤 명 근(Yoon, MyungKeun)
종신회원
1996년 2월 : 연세대학교 컴퓨터과학과 학사
1998년 2월 : 연세대학교 컴퓨터공학과 석사
2008년 12월 : University of Florida, 컴퓨터공학 박사
1998년 1월 ~ 2010년 2월 : 금융결제원 과장
2010년 3월 ~ 현재 : 국민대학교 컴퓨터공학부 조교수
<관심분야> 컴퓨터&네트워크 보안, 네트워크 알고리즘, 금융보안, randomized algorithm, 빅데이터