정 보 보 호 학 회 지
제24권 제3호, 2014. 6

인터넷뱅킹 키보드보안 기술의 안전성과 편의성

박 영 록*, 윤 명 근**

요 약

키보드는 전통적인 입력 장치로서 사용자가 입력하는 값을 컴퓨터 내부로 전달한다. 공격자들은 인터넷뱅킹 사용자들이 입력하는 키보드 값을 알아냄으로써 사용자의 비밀번호와 중요정보를 얻어낼 수 있는데, 이를 방어하기 위해서 다양한 키보드보안 기술이 제안되었으며 일부는 실제로 구현되어 사용되고 있다. 하지만 키보드보안 기술의 복잡도가 높아지면 보안성은 강화되더라도 사용자의 편의성을 저하시킬 수 있으며, 이러한 기술들은 현실 세계에서 활용되지 못한다. 본 논문에서는 인터넷뱅킹 키보드보안을 강화하기 위해서 제안된 다양한 기술들을 정리해보고, 키보드보안 기술의 편의성과 안전성에 대해서 살펴본다.

Ⅰ. 서 론

2014년 3월말을 기준으로 인터넷 뱅킹 서비스 등록 고객 수는 약 9,775만 명(중복 포함)으로 2013년 4/4분기 대비 2.4% 증가하였다. 스마트폰 뱅킹 등록자 수 또한 약 4,034만 명으로 빠른 증가세를 지속하고 있으며 2009년 12월 최초 서비스 개시 이후 최초로 4천만 명을 돌파하였다. 인터넷 뱅킹 일 평균 이용건수 및 금액은 각각 약 6,369만 건, 약 36조 1,394억 원으로 전 분기 대비 각각 14.7%, 3.9%가 증가하였다. 스마트폰 뱅킹의 경우는 약 2,737만 건, 1조 6,276억 원으로 전 분기 대비 각각 14.5%, 6.7% 증가하였다. [표 1]은 인터넷 뱅킹과 스마트 폰 뱅킹 고객 및 이용 실적을 보여준다[1].

스마트폰으로 전자금융거래를 사용하는 고객들은 시간과 장소에 제약 받지 않고 은행 업무를 이용 할 수 있다. 하지만 이러한 방식의 은행 업무 이용은 은행 창구에서 직접 수행하는 것에 비해 보안이 상대적으로 취약하다. 이러한 취약점을 보완하기 위해서 다양한 보안기술이 사용되고 있는데, 보안이 강화되는 반면 사용자의 편의성은 감소한다. 본 논문에서는 키보드를 통해서 입력되는 비밀번호와 중요정보의 유출을 차단하기 위해서 사용되고 있는 키보드보안 기술을 편의성과 안전성 측면에서 살펴본다.

〔표 1〕 인터넷 뱅킹 및 모바일 뱅킹 실적 (일평균)

<단위 : 천건, 십억원>

구분		2012년	2013년	2014년
건수	인터넷뱅킹	47,683	55,506	63,688
	스마트폰	15,346	24,462	27,597
금액	인터넷뱅킹	33,447	34,799	36,139
	스마트폰	1,134	1,573	1,663

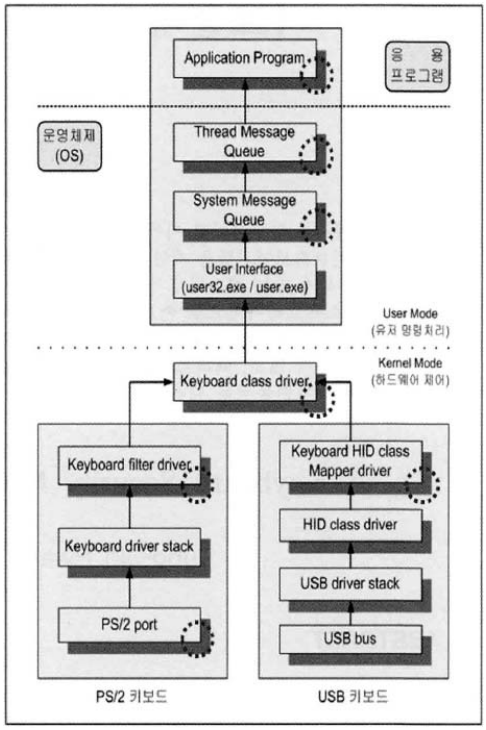
Ⅱ. 키보드보안 기술

2.1 키보드 암호화 기술

키보드 암호화 기술은 키보드보안솔루션으로 알려져 있을 만큼 대표적인 키보드보안 기술이다. 인터넷뱅킹 사용자는 은행에서 제공하는 키보드 암호화 프로그램을 PC에 설치한다. 키보드 암호화 프로그램은 사용자의 PC가 공격자에게 점령당하여 키로거(keylogger)나 화면캡처 기능을 수행하는 악성 프로그램이 실행되는 경우에 대비하여 키보드 입력으로부터 중요 정보가 노출되는 것을 막기 위해서 사용된다.

이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임
(no. 2013R1A1A1062412)
* 국민대학교 컴퓨터공학부 (yrpark@kookmin.ac.kr)
** 국민대학교 컴퓨터공학부 (mkyoon@kookmin.ac.kr)

키보드 암호화 프로그램이 설치되어 있지 않을 경우, 키보드 인터럽트 하이재킹, 키보드 드라이버 해킹, DLL 인젝션 해킹, 메모리 저장값 유출 등 여러 가지 방법으로 다양한 위치에서 키보드 입력 값 탈취가 가능하다[3]. 국내 키보드 보안 프로그램들은 탈취가 가능한 구간의 입력 값들을 암호화하여 데이터를 보호한다. 그리고 키로거가 입력 값을 가로채지 못하도록 더미 값을 상위단계로 올려 보내도록 되어있다. 이러한 방식으로 키보드 보안 프로그램은 사용자가 입력하는 중요한 정보를 암호화하여 정보 유출을 방지한다.



〔그림 1〕 키보드 입력정보 흐름에 따른 취약점〔2, 3〕

키보드 암호화 프로그램이 의도대로 정상적으로 동작하면, 키로거를 통한 사용자 입력 값 유출을 막아줄 수 있다. 하지만 공격자가 키보드 암호화 프로그램의 구동 자체를 인터넷뱅킹 접속 초기 단계에서 강제로 차단시키거나, 키보드 암호화 프로그램의 취약점을 이용해서 중요 정보만을 유출시키는 공격에 대해서는 약점이 있다. 이를 보완하기 위해서 개인 정보 입력 방식을 가상 키패드, 가상 키보드, 멀티채널 등과 조합하여 보안성을 높이는 연구가 진행되고 있다.

2.2 가상 키패드

인터넷뱅킹 서버는 키보드 입력 값 유출을 방지하기 위해서 화면에 가상 키패드를 나타내어 사용자가 마우스를 이용하여 입력 값을 클릭하도록 한다. [그림 2]는 국내 은행에서 제공하고 있는 가상 키패드 구동 화면이다. 모니터 화면의 가상 키패드 상에서 마우스 클릭을 이용하여 값을 입력하면 키보드를 통한 정보 유출을 막을 수 있다. 가상 키패드를 사용하면 마우스를 추가적으로 이용해야 하므로 사용자 편의성은 약간 낮아진다.

〔그림 2〕 인터넷 뱅킹 가상 키패드

최근에는 PC를 이용한 인터넷뱅킹 뿐 아니라 스마트폰을 이용하여 거래할 때에도 가상 키패드를 사용한다. [그림 3]은 스마트폰을 이용하여 인터넷뱅킹 거래를 할 때 사용하는 가상 키패드 화면이다. 새로운 거래가 발생할 때마다 혹은 새로 고침을 할 경우마다 키 위치가 변경된 새로운 키패드가 생성된다.

〔그림 3〕 스마트폰 가상 키패드(왼쪽)와 보안성을 강화한 키패드(오른쪽)〔4〕

일반적으로 스마트폰 뱅킹은 불특정 다수의 여러 사람이 모여 있는 장소에서도 사용될 수 있다. 이러한 장소에서 사용될 경우, 스마트폰 화면에서 키패드로 입력되는 내용을 사용자의 어깨 너머로 훔쳐보는 공격인 SSA(Shoulder Surfing Attack)가 성공적으로 수행될 수 있다.

[그림 3]의 오른쪽 화면은 기존의 스마트폰 가상 키패드의 SSA 약점을 개선하기 위해서 숫자들을 무작위로 생성하여 그리드 없이 화면에 나타내는 기술을 보여준다. [그림 3]의 오른쪽 그림처럼 정해진 포맷 없이 무작위로 숫자가 위치하는 기술을 사용하면, 공공장소에서의 보안성은 높아질 것으로 기대되지만 사용성은 떨어지는 것으로 설문조사 결과가 집계되었다[4].

2.3 패턴 비밀번호

스마트폰 뱅킹을 이용할 때, 텍스트 암호를 입력하는 대신에 사전에 설정해 놓은 특정 패턴을 입력하여 암호 대신 사용할 수 있다. [그림 4]는 현재 국내 은행 중 한 곳에서 제공하고 있는 패턴 비밀번호 사용방식을 보여준다.

[그림 4]의 왼쪽은 패턴 비밀번호를 입력 시 패턴에 해당하는 라인이 표시된다. 공공장소에서 SSA 공격에 취약할 수 있기 때문에 이를 개선하여 입력되는 라인을 시각적으로 표시하지 않음으로써 SSA 공격에 대한 방어력을 높이는 방식도 제공되고 있다([그림 4] 오른쪽 그림).

〔그림 4〕 스마트폰 패턴 비밀번호(왼쪽) 방식과 SSA 방어를 위한 방식(오른쪽)

2.4 동적 가상 키보드

주로 스마트폰에서 키보드 입력은 가상 키보드 기술을 사용해서 구현된다. [그림 5]는 스마트폰 뱅킹에서 사용되는 가상 키보드 화면이다. 화면을 통해서 사용자는 가상 키보드의 특정 키 값을 선택하게 되는데, 이때 공격자가 심어놓은 악성코드가 화면캡처를 수행하면 입력되는 정보가 공격자에게 쉽게 유출될 수 있다.

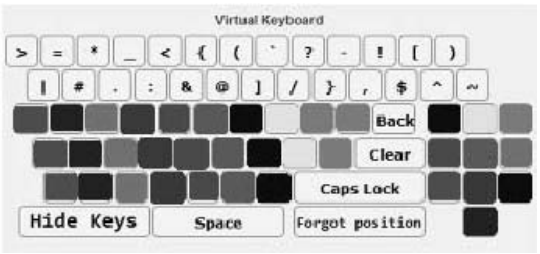
〔그림 5〕 스마트폰 뱅킹 가상 키보드

화면캡처 공격으로 인한 취약점은 가상 키패드를 포함한 모든 키보드 입력 방식에서 유효하다. 가상 키패드의 경우에는 새로운 거래마다 다른 배열의 키패드를 생성해 주지만, 그렇다고 해서 화면캡처 공격으로부터 안전할 수는 없다. 인터넷뱅킹의 가상 키패드를 사용하더라도 공격자는 마우스의 위치를 통해 값을 유추할 수 있으며, 이러한 상황에서 화면캡처 공격이 병행되면 손쉽게 입력정보가 유출될 수 있다.

화면 캡처 공격에 취약한 기존의 가상 키보드를 보완하기 위해서 M. Agarwal 등은 동적 가상 키보드 기법을 제안했다[5]. 동적 가상 키보드의 특징은 첫째, 키를 클릭 한 뒤 또 다시 키보드의 레이아웃을 변경한다. 둘째, 키 감추기를 통해 화면이 캡처당하더라도 키의 위치를 노출 시키지 않는다. [그림 6]은 동적 가상 키보드 기술의 구현 화면을 나타낸다.

〔그림 6〕 동적 가상 키보드[5]

현재 은행에서 스마트폰 어플리케이션에서 제공하는 가상 키보드처럼, 동적 가상 키보드의 키 위치는 임의적으로 생성된다. 하지만 사용자가 변화되는 키의 위치를 쉽게 기억 할 수 있도록 각 열은 서로 다른 색으로 표현한다. 사용자는 키의 위치를 기억한 뒤 “Hide Keys” 버튼을 클릭하여 키보드에서 키 값을 보이지 않도록 한다. [그림 7]은 “Hide Keys”를 클릭한 뒤 변화된 상태를 나타낸다. 그림과 같은 상태에서는 공격자가 화면을 캡처하더라도 키보드는 빈 공백 상태이므로 정보를 탈취할 수 없다. 사용자가 빈 공백 상태에서 비밀번호 한 자리를 클릭할 경우 키보드는 다시 랜덤으로 재배치된다. 이러한 과정을 반복하여 정보를 차례대로 입력한다.



〔그림 7〕 “Hide Keys”를 클릭하여 자판 배열을 감춘 화면〔5〕

동적 가상 키보드는 일반 가상 키보드에 비해서 화면 캡처에 의한 입력 값 유출 문제를 확실히 개선할 수 있다. 하지만 키 값을 하나 입력할 때마다 “Hide Keys”를 눌러서 자판을 재배열 시켜야 하므로 사용자 편의성이 크게 떨어지기 때문에 이 기술은 인터넷뱅킹과 같은 고객의 편의성도 중요한 환경에서는 사용되지 못하고 있다.

2.5 멀티채널 분산 키보드

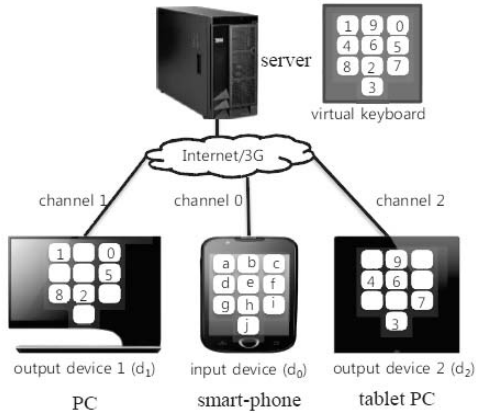
앞에서 살펴보았던 키보드 암호화, 가상 키보드, 패턴 비밀 번호, 동적 가상 키보드 기술은 사용자 입력 값을 키보드가 연결되어 있거나 구현되어 있는 컴퓨터에 전달하는 기술이다. 만약 컴퓨터 자체가 실력있는 공격자에 의해서 이미 점령되어 있는 상황이라면, 키로거, 화면캡처, 메모리 해킹 등의 기법으로 사용자 입력 값은 공격자에게 여전히 유출될 수 있다. 멀티채널 분산 키보드 기술은 앞선 기술들의 근본적인 문제를 해결해준다 [6].

멀티채널 분산 키보드 기술은 인터넷뱅킹 서버가 분산 키보드 자판을 생성하여 사용자의 서로 다른 디바이스로 키보드 자판을 구성하는 조각들을 나누어 전송해 줌으로써 모든 사용자 디바이스가 동시에 동일한 공격자에게 해킹당해 있지 않는 한 입력 값의 유출을 막아준다. 키보드 자판은 매 거래마다 새롭게 임의로 배열된다. 사용자 디바이스 중 한 대는 입력 기능을 전담하는데, 이 디바이스의 키보드 자판에는 아무 정보도 적혀있지 않다.

[그림 8]은 세 대의 사용자 디바이스가 참여하는 멀티채널 분산 키보드 시스템을 보여준다. 스마트폰을 입력 장치로 사용한다. 입력장치의 키보드에는 어떤 값도 화면에 표시되지 않는데, 설명의 편의를 위해서 `a’부터 `j’까지 문자를 표시했다. 멀티채널 분산 키보드의 동작 순서는 다음과 같다.

1) 서버는 임의의 키 배열을 갖는 가상 키보드를 생성한다.
2) 사용자가 사전에 등록한 출력 장치들로 가상 키보드 정보를 나누어 전송한다.
3) 사용자는 출력 장치들에 표시된 키 배열 정보를 보면서 입력 장치에 동일한 위치의 자판을 선택한다.

예를 들어서 입력 값이 “1234”라면 [그림 8]의 스마트폰을 통해서 “ahjd” 위치에 해당하는 자판 4개가 순서대로 클릭되어야 한다.



〔그림 8〕 멀티채널을 이용하여 분산된 가상 키패드〔6〕

멀티채널 분산 키보드는 출력 장치의 수가 많을수록 보안성이 높아진다. 동일한 공격자에게 입력 장치와 모든 출력 장치가 동시에 점령되지 않는 한 입력 값은 유출되지 않기 때문이다.

최근의 인터넷뱅킹은 보안성을 높이기 위해서 의도적으로 멀티채널을 사용하고 있다. 가장 대표적인 경우가 PC를 이용한 인터넷뱅킹에서 최종 확인을 위해서 사용자 핸드폰으로 전화를 걸어서 비밀번호를 추가로 입력받는 전화승인서비스이다. 최근에는 스마트폰, 태블릿 등 사용자가 보유하는 컴퓨팅 기기의 수도 증가하고 있기 때문에 멀티채널 분산 키보드를 다수 채널을 이용해서 구현하는 것이 가능해졌다.

일반적으로 편의성과 보안성은 반비례한다. 멀티채널 분산 키보드에서 출력 장치의 개수가 증가할수록 보안성은 강화되지만 사용자들의 불편함은 늘어난다. 사용하는 채널의 개수가 1개(입력 장치와 출력 장치가 동일한 일반 가상 키보드)부터 3개까지(입력 장치 1대, 출력 장치 2대) 사용자 편의성 테스트를 수행했다. 서로 다른 길이의 비밀번호를 입력할 때 소요되는 시간을 측정했는데, 채널수가 늘어날수록 많은 시간이 소요됨을 알 수 있다. [표 2]는 멀티채널 분산 키보드의 편의성을 측정하기 위해서 비밀번호 입력 시 소요되는 시간을 집계한 내용을 보여준다[6].

〔표 2〕 멀티채널 분산 키보드 비밀번호 입력 시간
(k:비밀번호 길이, 단위 : 초)

채널수	k=4	k=6	k=8	k=10	k=12
1	0.98	2.09	2.24	2.46	3.02
2	3.57	4.53	6.58	8.34	9.85
3	4.24	6.77	8.30	8.80	11.36

2.6 시각 인증 가상 키보드

Nyang 등은 최근에 키로깅 공격에 안전한 시각 인증 프로토콜을 제안했다[7]. QR(Quick Response) 코드와 PKI(Public Key Infrastructure)를 이용해서 안전하게 키보드 배열 정보를 사용자에게 전송한다. 프로토콜의 세부 동작 절차는 다음과 같다. 서버가 사용자의 공개키를 알고 있다고 가정한다.

1) 사용자는 터미널(PC, 노트북 등)에서 서버로 접근하기 위하여 로그인 ID를 입력하여 서버에 전송한다.
2) 서버는 임의로 배열된 가상키보드를 생성하고, 배열정보 Π를 사용자의 공개키로 암호화한다. 서버는 암호화된 배열정보를 QR코드로 변환하여 사용자 터미널로 전송하고, 터미널은 화면에 QR코드를 출력한다.
3) 사용자는 스마트폰을 이용해서 QR코드를 스캔한다. 스마트폰에 저장되어있는 사용자의 개인키로 배열정보 Π를 복호화 한다.
4) 스마트폰은 Π를 이용해서 키보드 배열을 화면에 보여준다.
5) 사용자는 스마트폰 화면의 키보드 배열을 보면서, 터미널에 표시된 더미 키보드의 동일 위치에 해당하는 자판 값을 인식한다. 터미널 키보드 상의 동일한 위치를 클릭하면서 비밀번호를 입력한다.

시각 인증 가상 키보드에서는 터미널 장치가 입력장치 역할을 담당하며, 스마트폰의 화면을 통해서 가상 키보드 배열을 사용자에게 보여준다([그림 9] 참조). Nyang 등은 동일한 논문에서 QR코드와 PKI를 이용하여 OTP (One-Time Password)를 안전하게 서버에서 사용자에게 전송하는 프로토콜도 제안했다[7].

〔그림 9〕 시각 인증 프로토콜을 이용한 가상 키보드 기법〔7〕

시각 인증 가상 키보드는 터미널과 스마트폰이 동시에 공격자에게 점령당하지 않는 한 입력 값이 유출되지 않는다는 점에서 멀티채널 분산 키보드 기술과 비슷한 안전성을 갖는다. 화면에 출력된 QR코드를 스캔해야

한다는 점에서 사용자 수고가 증가하기는 하지만, 향후 웨어러블 컴퓨팅과 스마트글래스 기술이 보급되면 사용 편이성이 향상될 것으로 기대된다.

Ⅲ. 결 론

본 논문에서는 인터넷뱅킹 키보드 보안기술을 안전성과 편의성 측면에서 살펴보았다. 악성코드에 감염되는 사용자 PC가 늘어남에 따라서 키보드 암호화 기술은 국내 모든 인터넷뱅킹에서 적용되고 있으며, 가상 키패드와 가상 키보드 기술도 폭넓게 사용되고 있다. 반면에 동적 가상 키보드와 멀티채널 분산 키보드, 시각 인증 가상 키보드는 높은 안전성을 보장하지만 편의성을 개선해야 실제 환경에서 적용될 수 있을 것으로 보인다. 향후에 개발될 키보드 보안 기술들은 보안성과 편의성을 동시에 만족시켜야 할 것으로 보이며, 최근에 발전하고 있는 스마트센싱, 웨어러블 컴퓨팅, 사물인터넷 기술 등을 접목시켜서 사용자로부터 정보입력을 받는 과정의 편의성을 높이는 연구가 추가적으로 필요할 것으로 예상된다.

참 고 문 헌

[1] 한국은행, “2014년 1/4분기 국내 인터넷뱅킹 서비스 이용현황”, 2014.5.15

[2] 황성진, 박경환, “서브클래싱 기반의 키보드 보안 기법”, 한국멀티미디어학회, 멀티미디어학회 논문지 제14권 1호, p15-23, 2011.1

[3] 금융 ISAC, “키보드 해킹기법 및 대응기술 분석”, 2005.11

[4] 안민서, 최준호, “모바일뱅킹의 비밀번호 입력방식 UI별 보안성, 사용성, 재미 인식 비교:공간맥락(공적, 사적 장소) 차이를 중심으로”, 한국HCI학회, p247-252, 2013.1

[5] M. Agarwal, M. Mehra, R.Pawar, D.Shah, “Secure authentication using dynamic virtual keyboard layout”, ICWET’11 Proceedings of the International Conference & Workshop on Emerging Trends in Technology, p288-291, 2011.2

[6] YoungLok Park, MyungKeun Yoon, “Distributed One-Time Keyboard Systems”, IEICE Transactions on Information and Systems, Vol.E96-D, No.12, 2013.12.

[7] DawHun Nyang, Aziz Mohaisen, Jeonil Kang, “Keylogging-resistant Visual Authentication Protocols”, IEEE Trans. on Mobile Computing, Vol.1, No.8, 2014.8

〈저 자 소 개〉

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

윤 명 근(Yoon, MyungKeun)
종신회원
1996년 2월 : 연세대학교 컴퓨터 과학과 학사
1998년 2월 : 연세대학교 컴퓨터 공학과 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