Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1219

스마트폰 환경에서 스파이웨어에 저항하는 동적 이미지 기반 가상 키보드 기법*

나 사 랑,† 권 태 경‡
연세대학교 정보대학원

A Rolling Image based Virtual Keyboard Resilient to Spyware on Smartphones*

Sarang Na,† Taekyoung Kwon‡
Graduate School of Information, Yonsei University

요 약

스마트폰 환경에서는 스마트폰의 개방성 및 휴대성의 특징으로 인하여 스파이웨어와 같은 악성 어플리케이션의 설치가 용이하며, 그 수가 크게 증가하고 있다. 스파이웨어는 개인 정보 유출 및 프라이버시 침해 등 심각한 보안 문제를 발생시키기 때문에 이를 위한 적절한 보안 기능을 제공하여 사용자의 민감한 정보를 보호해야 한다. 본 논문에서는 스파이웨어에 안전한 사용자 인증 기법을 제안한다.

ABSTRACT

Due to the fundamental features of smartphones, such as openness and mobility, a great deal of malicious software including spyware can be installed more easily. Since spyware can steal user's sensitive information and invade privacy, it is necessary to provide proper security mechanisms like secure virtual keyboards. In this paper, we propose a novel password input system to resist spyware and show how effectively it can reduce the threats.

Keywords: Smartphone, Authentication Method, Spyware, Secure Virtual Keyboard

I. 서 론

최근 스마트폰의 성능 향상으로 인하여 스마트폰 사용자 수가 크게 증가하였다. 스마트폰을 가지고 언제, 어디서든지 여러 업무를 처리할 수 있게 되었으며, 스마트폰 하나에 많은 정보를 저장하고 사용할 수 있게 되었다. 하지만 이와 동시에 스마트폰을 대상으로 스파이웨어(spyware)와 같은 악성 어플리케이션이 크게 증가하였으며, 이에 대한 많은 피해 사례가 보고되고 있다. 스파이웨어는 컴퓨터 시스템에서 사용자 몰래 개인 정보를 수집하는 악성 프로그램으로 스마트폰에서 모션 센서, 위치 정보 등을 수집할 수 있다[2]. 스파이웨어는 탐지하기 어렵고 제거하기도 힘들기 때문에, 한 번 설치되면 지속적으로 사용자 정보가 노출될 수 있는 위험이 존재한다. 특히 스마트폰과 같이 개방성 및 휴대성의 특징을 갖고 있는 컴퓨팅 장치는 악성 프로그램의 설치 경로가 다양하여 스파이웨어에 대한 위험이 더 크다. 이를 위해 사용자의 민감한 정보를 다루는 금융 어플리케이션은 자체적으로 랜덤 공백 키보드(Fig.1.)와 같은 보안 기능을 제공하고 있지만, 터치 이벤트와 스크린 캡쳐를 이용한 스파

접수일(2013년 10월 15일), 게재확정일(2013년 10월 21일)
* 본 연구는 미래창조과학부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)[10039180, 모바일 환경하에서 모바일 인증과 보안 강화를 위해 직관적이며 사용하기 편하고 안전한 인간-컴퓨터 상호작용(HCI) 기반 Usable Security 원천기술 개발]과 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업(NIPA-2013-H0301-13-1003)의 일환으로 수행하였음.
† 주저자, no.1.nasa@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

Fig.1. Random space keyboard[5]

이웨어에 안전하지 않다.

본 논문에서는 스파이웨어에 저항하는 패스워드 입력 기법인 RIK (Rolling Image virtual Keyboard, 릭)을 제안한다. 제안 기법은 터치 이벤트 정보와 스크린 캡처를 이용한 스파이웨어 공격에 안전하도록 설계되었다.

II. 관련 연구

금융 어플리케이션은 사용자의 안전한 비밀 입력을 위해 자체적으로 랜덤 공백 키보드를 제공하고 있다. 랜덤 공백 키보드는 QWERTY 배열을 사용하는 키보드 내에 임의의 공백을 삽입한 가상 키보드로 인증 시마다 매번 다른 키보드 레이아웃을 제공한다. 하지만 랜덤 공백 키보드는 문자키 위치만 조금 변경된 형태이기 때문에 터치 이벤트 정보를 통해 입력 비밀 값을 어느 정도 유추할 수 있으며, 스크린 캡처를 이용한 공격을 통해서는 확실히 알 수 있다.

스파이웨어로부터 사용자의 비밀 입력을 보호하기 위해 다양한 인증 기법들이 제안되었다. Lim은 안티 스크린 캡처 키패드를 제안하였다[3]. 이 기법은 랜덤 숫자 키패드에서 각 숫자의 부분 이미지를 빠른 리프레시(refresh) 속도로 번갈아가며 보여줌으로써 단일 스크린 캡처 공격을 사용하는 스파이웨어에 저항하고자 하였다. Agarwal 등은 동적 가상 키보드를 제안하였다[1]. 이 기법은 랜덤한 순서의 문자 배열을 사용하며, 패스워드를 입력할 때마다 문자 배열을 재정렬하여 보여준다. 사용자는 "Hide Keys" 버튼을 누른 후, 키보드 내의 문자들이 감춰지면 문자를 입력할 수 있다. 이를 통해 스파이웨어가 마우스 클릭 후, 화면을 캡처하는 공격으로부터 안전하게 하려고 하였다. 이 밖에도 일시적 비밀 값을 생성하여 패스워드를 간접적으로 입력하는 기법 등이 제안되었지만, 여전히 터치 이벤트 정보와 스크린 캡처를 이용한 스파이웨어에 안전하지 않으며, 특히 연속 스크린 캡처 공격에 취약하다.

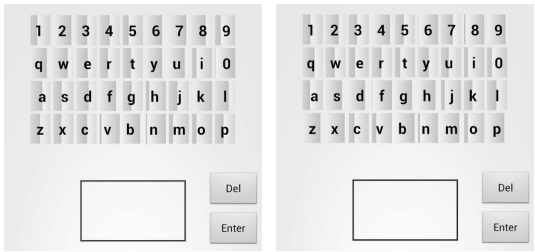

Fig.2. RIK prototype application

III. RIK

현재 스마트폰과 같은 터치스크린 기기에서는 문자 입력을 위해 가상 키보드를 제공하고 있다. 특히 가상 키보드는 다양한 웹 서비스에서 패스워드를 입력할 때도 자주 사용되는데, 민감한 사용자 정보를 입력하는 수단으로는 적절하지 않다. 본 논문에서 제안하는 RIK은 이동형 동적 이미지로 구성된 키보드 레이아웃을 사용하여 패스워드를 입력하게 함으로써 스파이웨어 공격으로부터 사용자의 비밀 정보를 보호할 수 있다.

3.1 개념

RIK에서 하나의 문자키는 문자와 지시자(indicator)로 구성된다. 지시자는 1개의 실제 지시자와 35개의 거짓 지시자로 구성되는데, 이 중에서 실제 지시자를 통해 패스워드를 입력하게 된다. 모든 지시자는 특정 방향으로 회전하는 이동형 동적 이미지를 갖으며, 각각의 동적 이미지들은 회전 속도와 시작 위치가 다르게 설정된다. 실제 지시자에서 동적 이미지는 왼쪽에서 오른쪽 방향 혹은 시계 방향으로 이동하고, 이와 반대로 거짓 지시자의 동적 이미지는 오른쪽에서 왼쪽 방향 혹은 반 시계 방향으로 이동한다. 이를 통해 RIK의 실행 과정을 실시간으로 볼 수 있는 사용자만이 실제 지시자의 위치를 쉽게 식별하여 문자를 입력하게 한다. 전체 키보드 레이아웃은 문자 레이아웃과 이미지 레이아웃으로 구성된다. 두 레이아웃은 서로 매치되어 겹쳐지는 형태로 구성되며, 문자 레이아웃이 고정된 이미지 레이아웃 위에 이동 가능한 스킨형 레이아웃으로 구성된다. 여기서 문자 레이아웃은 QWERTY 자판과 유사한 문자 배열로 구성된다. RIK 프로토타입 어플리케이션의 실행 화면은 Fig.2.와 같다.

3.2 입력 인터페이스

RIK은 문자 레이아웃을 이동하고 터치 동작을 해제하여 문자를 입력하는 입력 인터페이스를 사용한다[4]. 문자 레이아웃은 키보드 레이아웃 하단에 위치한 조작 패드를 가지고 이동하며, 조작 패드를 통해 움직인 거리는 특정 비율로 계산되어 키보드 레이아웃에 반영된다. 이러한 방식으로 문자 레이아웃을 이동하여 실제 지시자의 위치에 입력할 문자를 일치시키고, 화면에서 손을 떼면 해당 문자가 입력된다. 사용자는 문자 레이아웃을 직접 드래그하지 않음으로써 입력할 문자의 위치를 노출하지 않으며, 또한 상단의 문자 레이아웃을 쉽게 움직일 수 있다.

IV. 사용성 및 안전성 분석

RIK의 프로토타입 어플리케이션을 안드로이드 기반 스마트폰인 갤럭시 넥서스에서 구현하여 사용성 및 안전성 실험을 진행하였다. 사용성은 두 기법을 사용하는데 걸리는 실행 시간, 인증 성공/실패 여부, 백스페이스 횟수를 통해 분석하였으며, 일반 키보드와 함께 사용자 실험을 진행하였다. 안전성은 터치 이벤트 정보, 스크린 캡처를 이용한 스파이웨어 공격을 시뮬레이션하여 분석하였다.

4.1 사용성 분석

사용자 실험을 위해 QWERTY 자판에 익숙한 8명의 참가자(남자 5명, 여자 3명)를 모집하였다. 참가자들의 평균 나이는 27.5세이고, 휴대폰과 스마트폰 사용일은 각각 10.1년, 3.1년이다. RIK과 일반 키보드의 학습 효과를 줄이기 위해 사용자가 임의의 순서로 두 기법을 사용하도록 실험을 진행하였다. 참가자들은 두 기법의 사용 방법에 대해 설명을 듣고, 문자열 “abcd1234”를 가지고 세 번 연습하였다. 실제 실험에서는 각각 숫자와 소문자 알파벳 8자리로 구성된 시스템 패스워드와 사용자 지정 패스워드를 가지고 두 기법을 실험하였으며, 참가자들은 각각의 패스워드를 가지고 한 번 연습한 후, 사용성 평가를 위한 실험을 하였다.

4.1.1 실험 결과

RIK과 일반 키보드의 실험 결과는 Fig.3.과 같다. 일반 키보드의 평균 실행 시간은 사용자 지정 패스워드가 5.652초(sd: 1.298), 시스템 패스워드가 5.763초(sd: 0.796)이며, RIK의 평균 실행 시간은 시스템 패스워드가 20.825초(sd: 4.159), 사용자 지정 패스워드가 21.279초(sd: 3.191)이다. Repeated Measures-ANOVA 통계 테스트에서 기법 간 실행 시간이 유의함을 알 수 있었고($F(1,7) = 226.943$, $p < 0.001$), 패스워드 종류 간 실행 시간은 유의하지 않음을 알 수 있었다($F(1,7) = 0.07$, n.s.). 기법과 패스워드 종류 간 교호 작용은 유의하지 않았다($F(1,7) = 0.282$, n.s.). 두 기법 모두 인증에 실패한 세션은 없었으며, 일반 키보드에서 시스템 패스워드와 사용자 지정 패스워드를 입력할 때 각각 한 번의 백스페이스 입력이 있었다. 참가자들은 모든 실험이 끝나고 설문에 응답하였는데, 일반 키보드(mean: 4.63)가 RIK(mean: 2.5)보다 빠르다고 평가하였다.

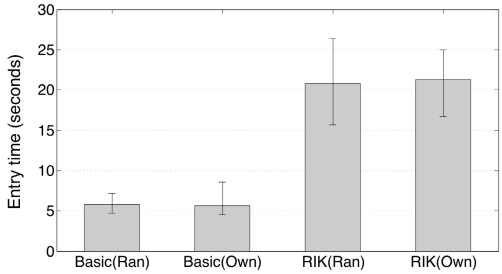

Fig.3. Usability experiment result

4.2 안전성 분석

RIK의 안전성 분석은 터치 이벤트 정보와 스크린 캡처 화면을 이용한 스파이웨어 공격을 시뮬레이션 하는 방식으로 진행하였다.

4.2.1 단일 스크린 캡처 공격

단일 스크린 캡처 공격에서는 문자 레이아웃을 이동한 후, 터치 동작을 해제할 때의 스크린 캡처 화면을 기록하여 입력 패스워드를 알아내고자 하였다. Fig.4.는 드래그 해제 시점에서 RIK의 키보드 레이아웃을 보여주고 있다. 실제 지시자의 위치는 ‘i’ 위치이며, 패스워드 ‘h’를 입력하기 위해 ‘i’ 문자키 위치로 문자 레이아웃을 이동하였다. 해당 화면만으로는 실제 지시자의 위치를 알 수 없기 때문에 사용자가 입력한 문자를 알 수 없다. 따라서 RIK은 단일 스크린 캡처 공격에 안전함을 알 수 있다.

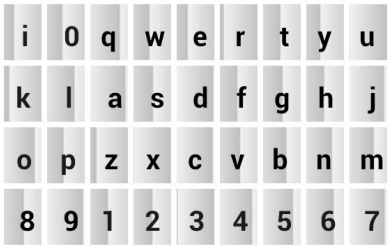

Fig.4. Single screen capture attack

4.2.2 연속 스크린 캡쳐 공격

연속 스크린 캡쳐 공격은 문자 레이아웃의 드래그 해제 시점 화면을 포함하여 특정 시간 간격으로 RIK의 실행 화면을 기록하는 방식으로 진행하였다. 1초 간격으로 연속적으로 화면을 캡쳐하여 입력 패스워드를 알아내고자 하였으며, Fig.5.는 패스워드 한 자리에 대한 스크린 캡쳐 화면을 보여주고 있다. 한 장의 드래그 해제 시점 화면을 포함하여 총 21장의 키보드 레이아웃 화면을 행 별로 나눠 겹쳐서 보여주고 있다. 각 행의 첫 번째 줄은 초기 실행 화면에서의 문자 위치이고, 마지막 줄은 드래그 해제 시점에서의 문자 위치이다. Fig.5.는 동적 이미지의 이동 패턴을 보여주고 있으며, 해당 정보를 가지고 실제 지시자의 위치와 입력 문자를 알아내고자 하였다. 문자키마다 다른 속성 값(시작 위치, 회전 속도)을 갖는 동적 이미지의 이동 패턴을 어느 정도 추측할 수 있었지만, 각각의 이미지가 어느 방향으로 얼마나 이동하는지는 알 수 없었다. 따라서 RIK은 연속 스크린 캡쳐 공격에도 안전함을 알 수 있다.

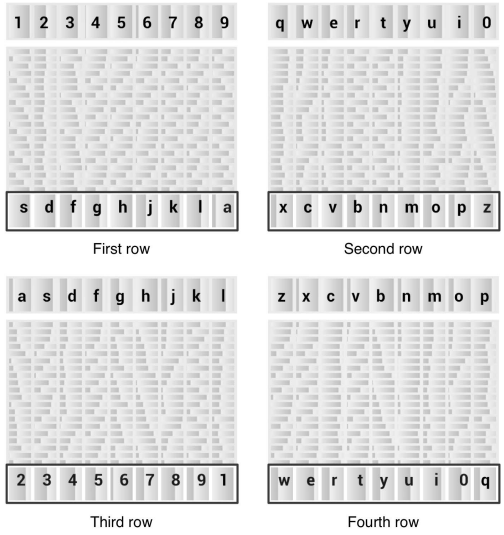

Fig.5. Successive screen capture attack

V. 결 론

본 논문에서는 RIK 인증 기법을 제안하였다. RIK은 실제 지시자를 이용하여 문자를 입력하는 방식을 사용함으로써 스마트폰 환경에서 스파이웨어로부터 사용자의 민감한 정보를 안전하게 입력할 수 있게 한다. 안전성 분석을 통해 실제로 스파이웨어 공격에 저항함을 알 수 있었고, 또한 사용자 실험을 통해 좋은 사용성을 제공함을 알 수 있었다. RIK은 스마트폰 환경의 다양한 어플리케이션에서 안전한 문자 입력 수단으로 적극 활용될 것으로 기대된다. 향후 고성능의 스파이웨어 공격에 대한 안전성 분석을 진행할 것이며, 사용성 또한 개선할 예정이다.

References

[1] M. Agarwal, M. Mehra, R. Pawar, and D. Shah, "Secure Authentication using Dynamic Virtual Keyboard Layout," Proceedings of the ICWET, pp. 288-291, Feb. 2011.

[2] L. Cai and H. Chen, "TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion," Proceedings of the HotSec, Aug. 2011.

[3] J. Lim, "Defeat Spyware With Anti-Screen Capture Technology Using Visual Persistence," Proceedings of the SOUPS, pp. 147-148, July 2007.

[4] T. Kwon, S. Na, and S. Park, "Drag-and-Type: A New Method for Typing with Virtual Keyboards on Small Touchscreens," Proceedings of the IEEE ICCE, pp. 460-461, Jan. 2013.

[5] woori smartbanking, http://www.woori-bank.com

〈저자소개〉

나 사 랑 (Sarang Na) 학생회원
2011년 2월: 세종대학교 컴퓨터공학과 학사
2013년 8월: 세종대학교 컴퓨터공학과 석사
2013년 9월~현재: 연세대학교 정보대학원 박사과정
〈관심분야〉 암호프로토콜, 스마트폰 보안, HCI 보안 등

권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc.
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 부교수
〈관심분야〉 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, HCI 보안 등