KIPS Tr. Comp. and Comm. Sys.
Vol.7, No.3 pp.73~80 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2018.7.3.73

Proposal and Implementation of Security Keypad with Dual Touch

Jinseok Song† · Myung-Woo Jung†† · Jung-In Choi††† · Seung-Hyun Seo††††

ABSTRACT

Due to the popularity of smartphones and the simplification of financial services, the number of mobile financial services is increasing. However, the security keypads developed for existing financial services are susceptible to probability analysis attacks and have security vulnerabilities. In this paper, we propose and implement a security keypad based on dual touch. Prior to the proposal, we examined the existing types of security keypads used in the mobile banking and mobile payment systems of Korean mobile financial businesses and analyzed the vulnerabilities. In addition, we compared the security of the proposed dual touch keypad as well as existing keypads using the authentication framework and the existing keypad attack types (Brute Force Attack, Smudge Attack, Key Logging Attack, and Shoulder Surfing Attack, Joseph Bonneau). Based on the results, we can confirm that the proposed security keypad with dual touch presented in this paper shows a high level of security. The security keypad with dual touch can provide more secure financial services, and it can be applied to other mobile services to enhance their security.

Keywords : Security Keypad, Simple Payment, Dual Touch, Mobile Banking

이중 터치를 이용한 보안 키패드 제안 및 구현

송 진 석† · 정 명 우†† · 최 정 인††† · 서 승 현††††

요 약

스마트폰의 대중화와 금융서비스의 간편화에 따라 모바일 금융 서비스를 이용하는 비중이 늘어나고 있다. 하지만 기존의 금융 서비스를 위해 개발된 보안 키패드는 확률 분석 공격이 가능하며 보안 취약성을 지니고 있다. 이에 따라 본 논문에서는 이중 터치를 기반으로 한 보안 키패드 제안하며 이를 구현하였다. 이에 앞서 국내 모바일 금융 서비스의 모바일뱅킹과 모바일 간편 결제 서비스에서 사용되는 기존 보안키패드의 종류를 알아보고 취약점을 분석하였다. 더불어 본 연구에서 제안한 이중터치보안키패드와 기존의 보안키패드의 안전성을 기존의 키패드 공격(Brute Force Attack, Smudge Attack, 키로깅 공격, 어깨너머공격, Joseph Bonneau)의 인증 프레임워크를 활용하여 비교하였다. 분석된 결과에 따라 본 논문에서 제안하는 이중 터치를 통한 보안 키패드가 높은 안전성을 보여줌을 확인할 수 있다. 이중 터치를 통한 보안 키패드를 활용하면 보다 안전한 금융서비스를 이용할 수 있으며 그 외 모바일 환경에서 이뤄지는 서비스에 적용하여 안전성을 높일 수 있다.

키워드 : 보안 키패드, 간편결제, 이중터치, 모바일 뱅킹

1. 서 론

현재 스마트폰의 대중화로 인해 금융거래 또한 모바일에 의존하는 비중이 늘어나고 있다. 2016년 말 한국은행이 발표한 자료에 따르면 국내 금융기관에 등록된 인터넷 뱅킹 고객 중 모바일뱅킹을 사용하는 고객이 61%이며 스마트폰 뱅킹 이용건수는 일평균 5,290만건으로 스마트뱅킹이 인터넷뱅킹 이용 증가세를 주도하고 있다[1]. 수치에서 알 수 있듯 이제 통장이나 카드를 들고 은행 창구를 방문하던 시대는 끝나가고 있다. 그동안 국내에서는 공인인증서 의무 사용 등과 같은 규제로 모바일 간편 결제 서비스 시장이 활성화되지 못했지만, 공인인증서 의무사용 폐지, PG사의 카드정보 저장 허용 등과 같은 금융 당국의 온라인 결제 정책 변화를 통해 2015년을 기점으로 모바일 간편 결제 서비스 시장이 부각되고 있다. TrendForce시장보고서에 따르면 2018년 모바일 간편 결제 서비스 시장의 규모는 약 9,300억 달러에 육박할 것으로 예상한다[2].

※ 이 성과는 2015년도 미래창조과학부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2015R1C1A1A01052491).
† 준 회 원 : 한양대학교 전자공학과 석사과정
†† 준 회 원 : 고려대학교 금융보안학과 석사과정
††† 준 회 원 : 한양대학교 공학기술연구소 전자공학과 박사후연구원
†††† 종신회원 : 한양대학교 전자공학과 부교수
Manuscript Received : August 23, 2017
First Revision : October 10, 2017
Accepted : October 16, 2017
* Corresponding Author : Seung-Hyun Seo(seosh77@hanyang.ac.kr)

모바일 금융 서비스가 활성화 되는 만큼 공격도 늘어나며 매년 악성코드가 증가하고 있다. 악성코드는 사용자의 스마트폰에 접근하고 내부 메모리에 저장되어 있는 인증서를 탈취할 수 있다. 또한 탈취된 인증서의 비밀번호와 모바일뱅킹 접근 계정정보를 탈취하기 위해 키로거(Keylogger)를 이용하여 사용자의 터치 좌표 값이 노출되고 키패드에 입력되는 정보의 탈취가 가능하기 때문에 매우 위협적이다[3]. 모바일 간편 결제 서비스의 경우에도 터치좌표 탈취 공격에 대한 보안 취약성에 우려가 있다[4]. 사용자의 편의성을 우선으로 결제 프로세스를 간소화하여 결제비밀번호만으로 결제가 가능하기 때문에 키로거로 인해 결제 비밀번호가 탈취된다면 바로 결제가 이루어지기 때문에 모바일뱅킹과 함께 보안 취약성으로 우려된다.

본 논문에서는 모바일 금융 서비스에 사용되는 보안키패드들의 종류를 조사해보고 보안취약성을 분석하여 기존의 보안키패드를 보완할 수 있는 키패드를 제안한다. 그리고 기존의 키패드의 보안 취약점을 분석하고 분석한 내용을 근거로 기존의 키패드보다 개선된 내용을 증명한다. 또한 제안하는 키패드의 안전성은 4가지 공격(Brute Force Attack, Smudge Attack, 키로깅 공격, 어깨너머공격(Shoulder Surfing Attack))에 대하여 비교분석하여 성능을 증명한다.

2. 스마트폰 보안 키패드 동향

일반적으로 스마트폰에는 기본적으로 안드로이드 운영체제에서 제공하는 키패드가 있지만 보안적인 면에서 취약하기 때문에 금융 어플리케이션의 경우 기본제공 키패드가 아닌 각 회사마다 자체 개발한 보안 키패드를 사용하고 있다. 현재 사용되고 있는 보안 키패드는 공백키패드, 랜덤키패드와 패턴키패드 등이 있다. Fig. 1은 현재 금융 어플리케이션에서 사용되고 있는 보안키패드의 인터페이스이다.

Fig. 1의 (a), (b), (c)는 공백 키패드를 기반으로 한 보안키패드이다. 공백 키패드의 특징은 일반 키패드와 숫자 배열은 같지만 중간에 랜덤으로 공백 두 개가 삽입되는 구조로 설계되어 있다. Fig 1의 (d)는 하나은행 어플리케이션에서 사용되고 있는 랜덤 키패드의 인터페이스이다. 랜덤 키패드는 기존의 안드로이드 운영체제에서 제공하는 기본키패드와 인터페이스는 유사하지만 숫자의 배열이 랜덤하게 이루어지는 특징을 가지고 있다. 랜덤으로 숫자를 배열하기 때문에 매번 사용 시마다 키패드는 숫자배열이 달라진다. 페이나우는 2016년 1월 4일 기준으로 국내에서 가장 많은 가맹점을 가지고 있는 간편결제 서비스이다. 또한 페이나우는 기존의 비밀번호 결제 이외에 '안전패턴', '그래픽 인증' 등을 결제 서비스에 최초로 도입한 국내의 중요 간편결제 서비스이다. Fig. 1의 (e)는 페이나우의 안전 패턴 키패드이며 패턴 기반 인증기법을 도입한 보안키패드이다. 하지만 기존 키패드에는 취약점이 존재한다. Table 1은 키패드 종류에 따른 취약점을 보여준다[5].

Fig. 1. Existing Security Keypad Interface, (a) Woori Bank, (b) Samsung Pay, (c) Kakao Pay, (d) KEB Hana Bank, (e) Paynow

Table 1. The Vulnerability of Each Keypad Type

Type of Keypad	Vulnerability
Blank Keypad	Brute force attack and key logging attack
Random Keypad	Brute force attack and Shoulder Surfing Attack
Pattern Recognition Keypad	Brute force attack and Smudge Attack

기존의 공백 키패드의 경우 키로깅 어플리케이션(Key logging Application)을 사용한 확률 분석에 취약함이 있다[4]. Fig. 2는 공백 키패드의 각 영역에 나타날 수 있는 숫자에 대한 확률을 나타낸 것이다[3].

Fig. 2. The Probability for the Number that can Appear in Each Area

Fig. 3. Smudge Attack on SmartPhone

Fig. 2에서도 알 수 있듯이 각 영역별로 숫자가 배치될 확률이 균일하지 않다. 즉, 공격자는 키로깅 어플리케이션을 이용해 수집한 좌표 값과 확률분석 알고리즘을 통해 사용자의 비밀번호를 쉽게 유추할 수 있다. 패턴 기반 보안 키패드는 현재 페이나우 서비스에서 사용자 인증에 사용하고 있다. 하지만 이러한 패턴 기반 보안 키패드의 경우 Smudge Attack에 취약하다[6].

Smudge Attack란 Fig. 3과 같이 사용자의 디바이스에 남아있는 얼룩을 분석하여 사용자가 패턴 인식 키패드에서 사용한 비밀 값을 알아내는 공격이다. 즉, Smudge Attack을 사용하여 패턴 인식 기반의 보안 키패드를 사용하는 모바일 뱅킹 사용자의 비밀 키를 유추해 낼 수 있다. 어깨너머공격은 어떤 사용자가 사무실이나 사람이 붐비는 장소에서 개인 기기를 사용하고 있는 경우, 사용자 주변에서 로그인이나 민감한 정보를 몰래 엿보는 것을 말한다[7]. 랜덤 키패드는 10개의 숫자 키를 랜덤하게 배열하여 키로깅 공격에 안전하지만 어깨너머공격에는 대응할 수 없으며 공격자가 사용자의 정보를 얻어 갈 수 있다[8].

3. 이중 터치를 통한 보안 키패드

기존에 사용되고 있는 키패드는 Brute force attack, 키로깅 공격, 어깨너머공격, Smudge Attack에서 취약점을 보이고 있기 때문에 이를 보완할 수 있는 키패드를 제안한다. 본 논문에서 제안하는 키패드는 키패드 마다 각각 2개의 숫자로 이루어져 이중성을 가지고 있는 멀티터치 키패드이다.

3.1 키패드 설계

키패드 설계에 있어서 중요한 부분은 이벤트 처리방식을 결정하는 것이다. 안드로이드에서는 클릭 이벤트, 키 이벤트, 터치 이벤트, 롱 클릭 및 포커스 이벤트 등의 이벤트가 처리되며, 이벤트 처리 절차는 모든 이벤트가 동일하다. 구현하려는 키패드의 이벤트 처리 절차는 Fig. 4와 같다.

키패드의 버튼에 실제 이벤트를 등록하기 위해서는 버튼 객체에 OnLongClickListener를 등록하고 View클래스 OnLong ClickListener의 onLongClick() 메소드에서 수행해야 할 로직을 넣어 주게 되면 이벤트 처리를 위한 작업이 진행된다.

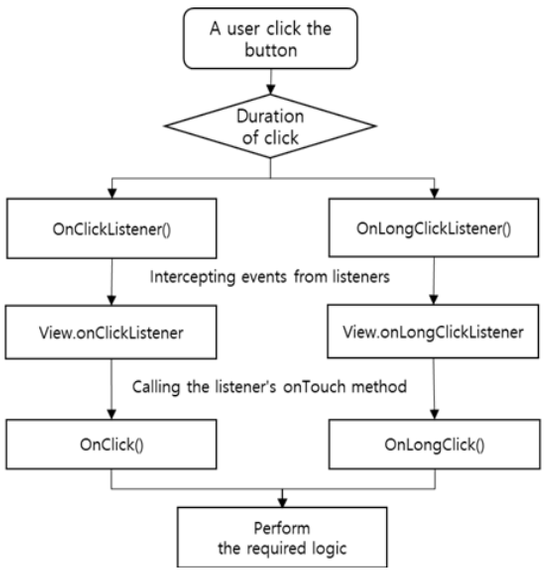


Fig. 4. Process of Dual Touch Keypad

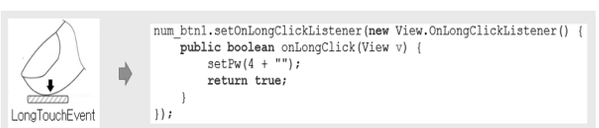


Fig. 5. LongTouchEvent Code

Fig. 6. ShortTouchEvent Code

숏클릭의 경우에도 같은 절차이다. 그럼 안드로이드 시스템의 숏클릭 이벤트 반응시간은 응용프로그램 내부 onClick() 함수의 1초미만 수행시간을, 롱클릭 이벤트의 반응시간은 onLongClick() 함수의 1초 이상 수행시간을 통하여 진행된다.

Fig. 5는 하나의 버튼에서 롱터치가 가능하도록 설계한 코드이다. 키패드의 레이아웃을 각각 num_btn1~num_btn10까지로 구성했다. 구성된 레이아웃에 각각 롱터치 모션을 주기 위해 롱클릭 리스너를 지정하는 메서드인 setOnLong ClickListener를 선언하고 롱클릭 이벤트 핸들러인 onLong Click이 발생되면 해당 이벤트가 발생되게 하여 롱터치모션을 구현할 수 있도록 코드를 구성하였다. Fig. 6은 숏터치가 구현 되도록 설계한 코드이며 숏클릭 리스너를 지정하는 메서드인 setOnClickListener을 선언하고 숏클릭 이벤트 핸들러인 onClick이 발생되면 해당 이벤트가 발생되게 하여 숏터치 모션을 구현할 수 있도록 코드를 구성하였다.

Fig. 7은 이중 터치로 설계된 버튼에서 두 가지 모션이 발생되었을 시 나타나는 상황의 예시이다. 사용자가 임의의 버튼(9/4)에 1초 이상 롱터치를 했을 경우 OnLong ClickListener()함수가 발생되고 롱터치 함수 내에 있는 이벤트가 발생되어

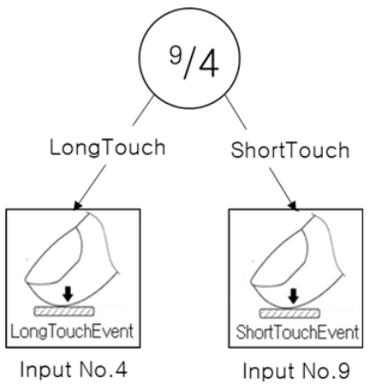


Fig. 7. Example of Dual Touch

사용자가 임의의 값으로 선택한 4가 입력되게 된다. 사용자가 1초미만 숏터치를 했을 경우 일반적인 OnClickListener()가 발생되기 때문에 숏터치 함수 내에 있는 이벤트가 발생되어 사용자가 임의의 값으로 선택한 9가 입력된다.

이 구조는 기존 키패드 모델과 동일하게 기본 라이브러리로 동작하게 되므로, 키패드의 성능적 오버헤드는 없다.

3.2 키패드 구현

본 실험은 모바일 금융 서비스에서 사용 중인 보안 키패드를 보완 할 수 있는 키패드를 개발하여 안전성을 분석하고 증명하기 위함이다. 실험 구현 환경은 Table 2와 같다.

Table 2. The Information of Experiment Environment

Device	SHW-M250S	SH-G920K
OS	Android 2.3	Android 5.1.1
Version	Gingerbread	Lollipop
Display	WSVGA(480 x 800)	QHD(2560 x 1440)

기존 키패드의 취약점은 비밀번호 입력 시 각 키가 특정 위치에 배치된다는 데에서 기인한다. 따라서 디바이스 터치 센서가 생성하는 터치 좌표 값 정보를 이용하는 악성 키로거앱을 통해 입력되는 패스워드를 알아낼 수 있는 가능성이 높다. 이러한 공격에 안전한 키패드는 패스워드 입력 시, 터치되는 버튼의 숫자 값 위치가 수시로 달라져야 한다.

Fig. 8은 제안하는 키패드가 구현된 형태이다. 사용자의 편의를 위해 유저 인터페이스형식은 기존의 키패드와 유사한 형태지만 각각의 버튼마다 두 개의 크고 작은 숫자로 구분시켜 구성했다. 큰 숫자는 롱터치, 작은 숫자는 숏터치이며, 구분된 숫자가 랜덤으로 구성되는 이중성을 가지고 있는 형태로 멀티 터치가 가능하다는 장점을 가지고 있다. 기존과 비교해보면, 키패드에서 '2, 3, 5, 7'이라는 비밀번호를 누른다고 가정하자. 일반키패드의 경우 두 번째 자리의 버튼에 있는 2를 선택하고 다음 숫자들인 3, 5, 7의 경우에도 항상 일정한 자리에서 선택하게 되므로 특정위치에 배치되는 취약성을 가지고 있다. 공백키패드의 경우에도 공백만

Fig. 8. Security Keypad with Dual Touch

추가되었을 뿐 일반키패드와 같은 방식으로 비밀번호를 입력하기 때문에 사용자 편의성은 높지만 보안성에서 각 키의 처음과 끝자리인 1, 9, 0이 배치되는 자리가 일정한 확률을 가지고 있으므로 비밀번호를 유추할 수 있는 취약성을 가지고 있다. 이보다 더 보안성이 강화된 랜덤 키패드는 기존 키패드와 인터페이스의 형식은 같지만 키패드의 숫자배열이 랜덤으로 배열되기 때문에 사용자가 입력할 때마다 숫자 값의 자리가 변경되어 사용자의 편의성은 이전 키패드들보다 떨어지지만 보안적인 면은 더 강화되어 있다. 하지만 이 랜덤 키패드도 하나의 버튼에 하나의 숫자 값만이 존재하기 때문에 어깨너머공격 등에서 쉽게 사용자가 입력하는 비밀번호를 탈취할 수 있다는 보안취약성을 보이고 있다.

본 논문에서 제안하는 키패드의 경우 이 부분까지 개선하여 설계된 구조이며 Fig. 8과 같이 하나의 버튼에서 숏터치와 롱터치가 구현되기 때문에 앞에서 가정한 비밀번호로 예를 들어보면 첫 번째 자리인 2를 숏자리와 롱자리 두 곳에서 선택할 수 있다. 또한 두 번째 자리인 3과 네 번째 자리인 7이 하나의 버튼에 존재하는 경우 '숏3', '롱7'과 '숏7', '롱3'의 경우로 두 개의 숫자 값을 선택할 수 있는 보안성을 가지고 있다. 그렇기 때문에 사용자가 어깨너머 공격 등을 통해 누르는 자리와 누르는 숫자를 확인하더라도 그 숫자가 어떤 숫자인지 확인이 불가능하다. 여기에 부가적으로 숫자가 이중으로 랜덤 배열된다. 이중 랜덤 배열이란 제안하는 키패드의 구조가 숏터치와 롱터치가 가능하여 하나의 버튼에서 두 개의 숫자 값을 입력할 수 있는 부분의 숏터치, 롱터치 부분 두 곳을 각각 랜덤 배열하게 설계하였기 때문이다. 이제, 구현된 제안하는 키패드에서 실제로 비밀번호를 가정하고 입력해본다.

Table 3은 제안하는 키패드에서 4자리의 비밀번호를 가정하고 테스트한 표이다. 비밀번호는 '3, 9, 5, 7'로 가정한다. 첫 번째 case 1에서는 숏3, 롱9, 숏5, 롱7의 경우로 선택하고 두 번째 case 2에서는 롱3, 숏9, 롱5, 숏7의 경우로 선택할 수 있다. 결론적으로 첫 번째 자리인 3이 하나의 버튼에서 선택될 경우의 수는 2가지이며 나머지 비밀번호'9, 5, 7'도 각각 2가지의 경우의 수가 되며 이 경우 종속사건으로 2^4이

Table 3. The Result of Password Input of Proposed Keypad

Number of Cases	Password (3, 9, 5, 7)			
Case 1	Short 3	Long 9	Short 5	Long 7
Case 2	Long 3	Short 9	Long 5	Short 7
Case 3	Long 3	Short 9	Short 5	Short 7
Case 4	Long 3	Long 9	Short 5	Short 7
Case 5	Long 3	Long 9	Long 5	Short 7
Case 6	Long 3	Long 9	Long 5	Long 7
Case 7	Short 3	Long 9	Long 5	Long 7
Case 8	Short 3	Short 9	Long 5	Long 7
Case 9	Short 3	Short 9	Short 5	Long 7
Case 10	Short 3	Short 9	Short 5	Short 7
Case 11	Short 3	Long 9	Long 5	Short 7
Case 12	Long 3	Short 9	Short 5	Long 7
Case 13	Short 3	Short 9	Long 5	Short 7
Case 14	Long 3	Long 9	Short 5	Long 7
Case 15	Short 3	Long 9	Short 5	Short 7
Case 16	Long 3	Short 9	Long 5	Long 7

다. 그럼으로 16가지의 경우의 7 수가 있으며 나머지 Case 3 ~ Case 16의 경우도 Table 3에서 확인할 수 있다.

4. 이중 터치를 통한 보안 키패드의 안전성 분석

본 절에서는 3절에서 제안한 키패드의 안전성을 분석할 것이다. 기존의 키패드에 대한 공격들에 대해서 제안한 키패드가 안전함을 보일 것이며 Joseph Bonneau가 제안한 인증 비교 프레임워크[9, 10]를 사용하여 편의성(Usability), 활용성(Deployability), 안전성(Security) 측면에서 기존 키패드와 비교 및 분석할 것이다.

4.1 Brute Force Attack

공백 키패드, 랜덤 키패드, 패턴 인식 키패드는 Brute Force Attack에 취약하다. 공백 키패드와 랜덤 키패드가 4자리의 비밀번호를 사용한다고 가정하면 각 자리에 들어갈 수 있는 경우의 수는 10가지이다. 즉, 4자리의 가능한 비밀번호의 총 경우의 수는 총 $10^4 = 10{,}000$개이다. 이는 전수조사 공격에 의해 비밀번호를 쉽게 유추할 수 있음을 말한다. 하지만 제안한 키패드의 경우 비밀번호의 각 자리마다 0~9 숫자와 각 숫자에 대응하는 롱터치, 숏터치의 경우가 존재한다. 즉, 가능한 키 공간은 아래 Equation (1)과 같다.

$$Key = \{0(S), 0(L), 1(S), 1(L), 2(S), 2(L), 3,(S), 3(L), ..., 8(S), 8(L), 9(S), 9(L)\} \quad (1)$$

한 자리에 들어갈 수 있는 키 번호의 수는 $|Key| = 20$가지가 된다. 제안한 키패드에서 4자리 비밀번호를 만들 수 있는 경우의 수는 $20^4 = 160{,}000$으로 기존보다 가능한 비밀번호의 집합이 $2^4 = 16$배 증가한다. 만약 비밀번호의 길이를 n이라 한다면 제안한 키패드의 가능한 비밀번호 집합은 기존의 키패드 보다 2^n배 증가하므로 비밀번호가 길어질수 록 전수조사공격에 상대적으로 강력해진다.

4.2 Smudge Attack

본 논문에서 제안한 키패드는 패턴 인식 키패드뿐만 아니라 공백 키패드와 랜덤 키패드 보다 Smudge Attack에 상대적으로 안전하다. 예를 들어 사용자가 '1234'를 비밀번호로 사용한다 하자. 사용자는 '1234'를 입력하기 위해서 각 숫자가 위치에 있는 패널을 터치할 것이다. 패턴 인식 키패드의 경우 사용자의 Smudge를 분석하여 비밀번호를 쉽게 유추할 수 있으며 공백 키패드는 확률분석을 통해 비밀번호를 유추할 수 있다. 또한 랜덤 키패드의 경우 공격자는 Smudge 를 통해서 사용자가 터치한 지점을 알 수 있으므로 최대 $\frac{1}{10}\times\frac{1}{9}\times\frac{1}{8}\times\frac{1}{7}\times 100 = 0.01984\%$의 낮은 확률로 비밀번호를 유추할 수 있다. 하지만 본 논문에서 제안한 키패드의 경우 전면 키패드와 후면 키패드가 랜덤하게 재배열되므로 Smudge Attack에 안전하며 랜덤 키패드보다 낮은 확률로 공격자가 비밀번호를 유추할 수 있다. 랜덤 키패드의 경우 각 자리의 숫자만을 유추하면 되지만 제안한 키패드의 경우 숫자와 터치 시간 또한 유추를 해야 한다. 제안한 키패드는 비밀번호의 길이가 n이라 할 때, 랜덤 키패드보다 Smudge Attack에 2^n배 안전성을 가진다 할 수 있다.

4.3 키로깅 공격(Key Logging Attack)

공백 키패드와 패턴 인식 키패드의 경우 키로깅 공격에 취약하다. 사용자가 랜덤 키패드를 사용하는 경우 공격자가 사용자 기기의 좌표 값을 탈취하여 4자리의 비밀번호를 유추할 수 있는 확률은 위의 Smudge Attack에서 분석한 것과 같이 최대 0.02%이다. 안전성을 분석하기에 앞서 공격자가 제안한 키패드의 전면 패드의 k번째 자리의 비밀번호를 유추할 사건을 A_k라 하며 후면 패드의 k번째 자리의 비밀번호를 유추할 사건을 B_k이고 k번째 자리의 비밀번호를 유추할 사건을 C_k라 하자. 즉, $P(A_1 \cap B_2 \cap B_3 \cap A_4)$는 사용자가 비밀번호를 (숏, 롱, 롱, 숏)하게 눌렀을 때 공격자가 비밀번호를 유추할 확률을 나타내며 $P(C_1)$은 이전의 랜덤 키패드에서 첫 번째 자리의 비밀번호를 유추할 확률이다.

공격자가 '5(S), 6(S), 7(L), 3(L)'을 비밀번호로 사용하고 제안한 키패드를 키패드로 사용하는 사용자의 비밀번호를 키로깅 공격을 통해서 유추한다고 가정하자. 이때 키로거는 사용자가 키패드를 짧게 눌렀는지 길게 눌렀는지를 구분할 수 있다. 이때 공격자는 터치 좌표가 <1, 3>, <2, 1>, <2, 1>, <1, 1>이며 (숏, 숏, 롱, 롱)임을 알 수 있다. 이 정보를 가지고 공격자가 비밀번호를 유추할 확률을 생각해보자. 먼

저 $P(A_1)=\frac{1}{10}$임을 알 수 있으며, $P(A_1\cap A_2)=\frac{1}{10}\times\frac{1}{9}$이다. 즉, 공격자가 사용자의 4자리 비밀번호를 유추할 수 있는 확률은 $P(A_1\cap A_2\cap B_3\cap B_4)=\frac{1}{10}\times\frac{1}{9}\times\frac{1}{10}\times\frac{1}{9}$이다. 이는 0.012%로 기존의 랜덤 키패드보다 약 0.008%낮은 확률이다. 만약 비밀번호의 자리가 6자리인 경우 랜덤 키패드에서 공격자가 사용자의 비밀번호를 유추할 확률은 최대 0.00066%이며 제안한 키패드에서 공격자가 6자리의 비밀번호를 유추할 확률은 최대0.00019%로 확률이 약 $\frac{1}{3}$배 감소한다. 이는 제안한 키패드가 공백 키패드와 패턴 인식 키패드보다 키로깅 공격에 강력하며 랜덤 키패드보다 높은 안전성을 가지고 있음을 알 수 있다.

4.4 어깨너머공격(Shoulder Surfing Attack)

기존의 키패드는 Shoulder Surfing Attack에 취약하다. 사용자가 비밀번호를 입력할 때 공격자는 사용자 주변에서 비밀번호를 몰래 엿보아 사용자의 비밀번호를 탈취할 수 있다[8]. 하지만 제안한 키패드의 경우 사용자가 비밀번호를 입력할 때 Long Touch와 Short Touch로 나누어지므로 공격자가 사용자의 입력 과정을 엿본다 하더라도 공격자는 사용자의 비밀번호를 탈취할 수 없다. 사용자가 (1,1), (2,3)을 터치하고 공격자는 사용자의 터치 좌표를 어깨너머 공격을 통해 탈취했다 가정하자. 공격자는 사용자의 터치 좌표로부터 사용자가 (1, 1)에서는 1 또는 3을 터치했다는 것을 알 수 있고 (2,3)에서는 0 또는 2를 터치했음을 알 수 있다. 하지만 공격자는 사용자가 정확이 어떤 비밀번호를 눌렀는지 알 수 없다. 즉, 공격자가 어깨너머 공격을 통해 사용자의 터치좌표를 알아낸다 하더라도 2^n만큼의 경우의 수를 생각해야 한다.

4.5 Joseph Bonneau 인증 비교 프레임워크를 통한 안전성 분석

본 절에서는 앞서 살펴본 키패드를 사용한 인증 기법들을 Joseph Bonneau[9]가 제안한 인증 비교 프레임워크를 이용하여 안전성 측면에서 비교 분석한다. 분석에 앞서 Joseph Bonneau에서 안전성을 분석하기 위해 제안하는 속성들은 물리 관찰 저항성, 사용자 위조 저항성, 추측 공격 저항성, 내부 관찰자 저항성, 정보 노출 저항성, 피싱 공격 저항성, 도난 저항성, 인증기관 부재, 명확한 사용자 동의, 비연결성이 있다. Table 4는 각 속성에 따른 안전성 만족 여부에 대한 결과이다. (a)는 공백 키워드, (b)는 랜덤 키패드, (c)는 패턴 인식 키패드, (d)는 본 연구에서 제안하는 키패드이다.

- S1(물리 관찰 저항성) : 본 항목은 어깨너머 공격과 같은 물리적인 관찰에 의한 공격에 안전해야 한다는 조건이다. 제안하는 키패드를 제외한 다른 키패드의 경우 사용자 인증 시 물리 관철에 의한 공격에 취약하다. 제안하는 키패드를 이용한 인증의 경우 물리 관찰 저항성을 만족한다.

Table 4. Safety Comparison and Analysis of Keypad (○ : satisfied, ×: unsatisfied)

Attribute	(a)	(b)	(c)	(d)
S1: Resilient to Physical Observation	×	×	×	○
S2: Resilient to Targeted Impersonation	○	○	○	○
S3: Resilient to Throttled Guessing	○	○	○	○
S4: Resilient to Unthrottled Guessing	×	×	×	×
S5: Resilient to Internal Observation	×	○	×	○
S6: Resilient to Leaks from Other Verifiers	×	×	×	×
S7: Resilient to Phishing	×	○	×	○
S8: Resilient to Theft	○	○	×	○
S9: No Trusted Third Party	○	○	○	○
S10: Requiring Explicit Consent	○	○	○	○
S11: Unlinkable	○	○	○	○

- S2(사용자 위조 저항성) : 본 항목은 사용자의 정보(생일, 이름 등)로부터 사용자로 위조가 불가능해야 한다는 조건이다. 본 논문의 키패드를 사용한 인증 기법들은 사용자의 정보를 사용하지 않기 때문에 해당 항목을 만족한다.
- S3 (추측 공격 저항성) : 본 항목은 공격자의 계산 능력에 한계가 있을 때 공격성에 대한 저항성을 알아본다.
- S4(비한계 추측공격 저항성) : 본 항목은 공격자의 계산 능력에 한계가 없을 때 공격성에 대한 저항성을 알아본다. 기존의 키패드와 제안한 키패드는 모두 본 항목을 만족하지 않는다.
- S5 (내부 관찰자 저항성) : 본 항목은 공격자가 사용자 디바이스 내부에서 인증에 관한 정보들을 습득하였을 경우 또는 도청에 안전해야 한다는 조건이다(e.g., by key-logging malware). 제안하는 키패드를 제외한 다른 키패드의 경우 내부 관찰자에 대한 저항성을 가지고 있지 못하기 때문에 제안하는 키패드만 본 항목을 만족한다.
- S6 (정보노출 저항성) : 본 항목은 여러 증명 기관이 있는 환경에서, 한 증명 기관에서 노출된 정보에 의해 다른 증명 기관의 인증에 피해가 없어야 한다는 조건이다. 본 인증 기법들은 해당 항목을 만족하지 않는다.
- S7 (피싱공격 저항성) : 본 항목은 피싱 공격에 대해서 안전해야 한다는 조건이다. S5 항목과 같은 이유로 제안하는 기존의 키패드들은 본 항목을 만족하지 않지만 제안한 키패드는 본 항목을 만족한다.
- S8 (도난 저항성) : 본 항목은 사용자의 장비를 습득한 자가 인증을 시도할 시 성공하기 어려워야 한다는 조건이다. 패턴 인식 기반 인증 기법의 경우 Smudge Attack에 취약 하므로 본 항목을 만족하지 않는다. 패턴 인식 기반을 제외한 키패드들은 공격자가 사용자의 장비를 습득했다 하더라도 패스워드를 알지 못하면 인증이 어렵기 때문에 본 항목을 만족한다.
- S9 (인증기관 부재) : 본 항목은 신뢰할 수 있는 제 3의 인증기관이 없는 환경에서 안전성을 보장해야한다는 조건이다. 본 논문의 키패드들의 경우 제 3의 인증기관이

필요하지 않기 때문에 해당 항목을 만족한다.

- S10 (명확한 사용자 동의) : 본 항목은 사용자 인증 시 사용자의 동의가 필요하다는 조건이다. 본 논문의 키패드들은 사용자 인증을 위해 패스워드를 이용한 사용자 동의가 필요하기 때문에 본 항목을 만족한다.
- S11 (비연결성) : 본 항목은 여러 개의 제 3의 기관을 사용할 경우 각 기관사이의 어떠한 연결성도 존재해서는 안 된다는 조건이다. S9의 항목과 마찬가지로 제 3의 기관을 사용하여 인증을 수행하지 않기 때문에 본 항목을 만족한다.

4.6 제안하는 키패드의 편의성 분석

본 절에서는 기존의 키패드와 제안하는 키패드의 편의성 측면을 분석한다. 전체적으로 분석해보았을 때 제안하는 키패드의 경우 사용자가 비밀번호를 기억해야하는 측면에서는 기존의 키패드들과 큰 차이가 없으며 비밀번호를 입력할 시에 조금의 절차가 추가될 뿐 기존과 큰 차이가 없다.

기본적으로 제안하는 키패드의 경우 패스워드를 입력하는 과정에서 랜덤 키패드보다 다소 느린 절차가 포함될 뿐 편의성 측면에서 그 성격이 유사하여 사용자 편의성에 큰 차이가 없다 . 그리고 공백 키패드와 비교해보았을 때, 제안하는 키패드의 경우 사용자가 자신의 비밀번호를 입력하기 위해 번호를 찾아야하는 절차를 포함하지만 같은 길이의 비밀번호를 기억한다하였을 때, 사용자의 포인터 위치 이동에 걸리는 시간은 비슷하여 그 차이가 크지 않다. 패턴 인식 키패드의 경우 제안하는 키패드보다 기억하기는 쉬우나 입력시간에는 큰 차이가 없으므로 사용자 편의성 측면에서 큰 차이가 나타나지 않는다.

5. 결 론

모바일 금융 서비스에서 가장 중요한 부분 중 하나는 보안 키패드이다. 현재까지의 보안키패드는 디바이스의 터치센서를 통해 터치 좌표 값을 탈취할 수 있는 키로깅이 구현된다면 이를 통해 여러 차례 수집한 비밀번호 인증 정보를 이용하여 확률 분석 공격이 가능하며 사용자의 비밀번호가 탈취될 수 있는 보안취약성을 가지고 있다. 하지만 제안하는 키패드는 이중터치를 추가함으로써 추측공격 확률을 기존보다 낮출 수 있는 장점이 있다. 즉, 안전성 분석을 통해서 알 수 있듯이 제안된 키패드는 기존의 키패드 보다 안전하다. 또한, 제안하는 키패드는 기존의 키패드와 비교한때 Smudge Attack과 키로깅 공격에서 매우 안전하다. 이 연구를 통해 제안한 키패드는 안전하게 모바일 금융 서비스를 이용할 수 있는 환경을 제공한다는 점에서 가치가 있다.

References

[1] The Bank of Korea, “Domestic Internet banking service usage in 2016,” 2017.

[2] TrendForce, “Total Revenue of Global Mobile Payment Market,” 2016.

[3] Y. H. Lee, “An Analysis on the Vulnerability of Secure Keypads for Mobile Devices,” *The Journal of Internet Computing and Services*, Vol.14, No.3, pp.15-21, 2013.

[4] J. S. Song, M. W. Chung, S. H. Seo, and S. H. Lee, “Security vulnerability analysis of Simple Mobile Payments Services,” *The Korea Information Processing Society Fall Conference*, Vol.22, No.2, pp.817-820, 2015.

[5] I. Kim, “Keypad against brute force attacks on smartphones,” *IET Information Security*, Vol.6, No.2, pp.71-76, 2012.

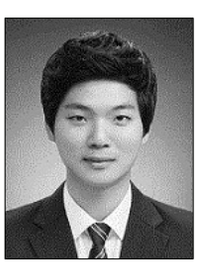
[6] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge Attacks on Smartphone Touch Screens,” *Proceedings of the 4th USENIX Conference on Offensive Technologies*, Washington, DC, pp.1-7, August 09, 2010.

[7] J. Long, J. Wiles, S. Pinzon, and K. D. Mitnick, “No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing,” Rockland, MA: Syngress, pp.27-60, 2008.

[8] S. H. Kim, M. S. Park, and S. J. Kim, “Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes,” *Journal of the Korea Institute of Information Security and Cryptology*, Vol.24, No.6, pp.1159-1174, 2014.

[9] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 553-567). IEEE, 2012.

[10] H. J. Shin and J. B. Hur, “Pattern-Based User Authentication System Research Trend and Comparison,” *Journal of the Korea Institute of Information Security and Cryptology*, Vol.25, No.3, pp.36-43, 2015.



송 진 석

http://orcid.org/0000-0002-4287-5660

e-mail : jssong90@hanyang.ac.kr

2017년 고려대학교 정보수학과(이학사)

2018년～현 재 한양대학교 전자공학과 석사과정

관심분야 : Security Protocol Design & Authentication

정 명 우

http://orcid.org/0000-0002-9293-1915

e-mail : jung4651@korea.ac.kr

2017년 고려대학교 정보수학과(이학사)

2017년～현 재 고려대학교 금융보안학과 석사과정

관심분야 : Financial Security & Cryptography

최 정 인

http://orcid.org/0000-0003-2959-2268
e-mail : peach0206@hanyang.ac.kr
2010년 가천대학교 컴퓨터미디어학과 (공학사)
2012년 이화여자대학교 컴퓨터공학과 (공학석사)
2017년 이화여자대학교 컴퓨터공학과(공학박사)
2017년～현 재 한양대학교 공학기술연구소 전자공학과 박사후연구원
관심분야 : Sensor, IoT, Authentication

서 승 현

http://orcid.org/0000-0002-1150-7080
e-mail : seosh77@hanyang.ac.kr
2000년 이화여자대학교 수학과(이학사)
2002년 이화여자대학교 컴퓨터학과 (공학석사)
2006년 이화여자대학교 컴퓨터학과 (공학박사)
2006년～2010년 금융보안연구원 주임연구원
2010년～2012년 한국인터넷진흥원 선임연구원
2014년～2015년 고려대학교 정보보호대학원 BK21+ 사업단 연구교수
2015년～2016년 고려대학교 수학과 조교수
2017년～현 재 한양대학교 전자공학과 부교수
관심분야 : Front-end Design & Verification Methodology