Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.4, Aug. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.4.731

원타임 키패드의 보안성 분석*

김 종 락,†‡ 이 나 리, 노 영 건, Lucky Erap Galvez
서강대학교 수학과

A Study on the Security of One-Time Keypad (OTK)*

Jon-Lark Kim,†‡ Nari Lee, Young Gun Roe, Lucky Erap Galvez
Department of Mathematics, Sogang University

요 약

보안에 관한 많은 암호 기술의 도입에도 불구하고 어깨 넘어 훔쳐보기 등과 같은 사회공학적인 공격은 원천적으로 차단하기 어려운 공격기법이다. 현금자동입출기기와 같이 개방된 공간에 설치된 금융시설에서는 더욱 그러한 공격을 차단하기 어렵다. 이뿐 아니라 업무처리 비중이 점점 늘고 있는 온라인 금융 서비스는 공간의 제약 없이 어디서나 사용가능하다는 편리성의 이면에 어깨 넘어 훔쳐보기, 스머지 공격, 구글 글라스를 이용한 비밀번호의 위치점 유추 등의 공격에 취약한 부분이 있다. 본 논문에서는 현금자동입출기기와 인터넷 뱅킹에서 원타임 키패드(One-Time Keypad)를 사용함으로 비밀번호 유출에 안전함을 보이고, 기존에 사용되는 키패드와 OTP (One-Time Password)와의 보안성을 비교 분석하였다.

ABSTRACT

For all the various cryptographic techniques related to security, social technological attacks such as a shoulder surfing are infeasible to block off completely. Especially, the attacks are executed against financial facilities such as automated teller machine(ATM) which are located in public areas. Furthermore, online financial services whose rate of task management is consistently increasing are vulnerable to a shoulder surfing, smudge attacks, and key stroke inference attacks with google glass behind the convenience of ubiquitous business transactions. In this paper, we show that the security of ATM and internet banking can be reinforced against a shoulder surfing by using One-Time Keypad(OTK) and compare the security of OTK with those of ordinary keypad and One-Time Password(OTP).

Keywords: One-Time Keypad, OTK, OTP, password, security

I. 서 론

전자 상거래가 오프라인에서 온라인으로 확대되면서 자연스럽게 비밀번호의 중요성이 대두되어 왔다. 한국은행에 따르면 2016년 3/4분기 기준으로 현금자동입출기기의 업무처리 비중은 36.2 %, 인터넷 뱅킹은 42.7 %로 전체 금융 업무의 78.9 %를 담당하고 있다[1]. 그리고 이에 대한 보안을 위해 그동안 많은 암호 기술이 도입되었으나 사회공학적 공격에 대해서는 여전히 안전하지 않은 상황이다. 2016년 정보보호 실태조사 결과를 살펴보면 개인 부문에서 침해사고 경험은 전체 조사자의 17.4 %로, 전년에 대비해 3.9 %가 증가하였고 이 중 개인정보 유출 및 사생활 침해는 9.2 %를 차지하는 것으로 나타났다[2].

특히 전자금융 거래는 비대면성의 특성에 의해 여러 공격 위협이 존재할 수 있으므로, 각 단계마다 거래에 대한 안전성을 보장해야 한다. 이에 대해 금융

Received(03. 23. 2017), Modified(06. 21. 2017), Accepted(06. 29. 2017)
* 본 연구는 한국연구재단 서강대 LINC 연구과제(201680055.01) 지원으로 수행하였습니다.
† 주저자, jlkim@sogang.ac.kr
‡ 교신저자 jlkim@sogang.ac.kr(Corresponding author)

보안 연구원의 암호기술 활용 가이드에는 이용자의 입력정보 보호, 거래 시 추가인증 수단(OTP, 인증서 등), 전송정보 보호 등의 기술이 적용되어야 한다고 나와 있다[3]. 이는 현금자동입출기기나 인터넷 뱅킹의 경우에도 사용자의 비밀번호 정보가 보호되어야 함을 의미한다.

현재 범용되는 숫자 키패드는 현금자동입출기기, 인터넷 뱅킹, 온라인/모바일 결제, 도어락 등 다양한 곳에 사용되고 있다. 이 중 금융 업무 처리에 가장 많이 사용되는 인터넷뱅킹이나 현금자동입출기기 같은 경우 키패드에 비밀번호 입력 시 어깨 넘어 훔쳐보기, 스머지, 구글 글라스를 이용한 비밀번호의 위치점 유추 등의 공격에 취약하다는 것이 알려져 있다([4],[5],[6]). 어깨 넘어 훔쳐보기 같은 비기술적 공격의 근원적인 문제는 키패드에 비밀번호를 입력하여 사용자 인증을 하는 과정이 공공장소에서 이루어진다는 점이다.

이런 여러 공격에 대응하고자 그동안 많은 연구가 이루어져 왔다. 전수조사에 강한 키패드로 랜덤 키패드가 제안되었고[7], 스마트폰 혹은 스마트패드 상에서 구글 글라스 같은 스마트 디바이스의 공격도 효율적으로 방어할 수 있는 입력 위치 유추 방지를 위한 보안 키패드도 제안되었다[6]. 이 외에 어깨 넘어 훔쳐보기 공격에 대응하기 위한 연구도 많이 진행되어 왔다. 사람의 색 인지능력의 한계를 이용한 오라클 기반 멀티 라운드 프로토콜을 이용한 PIN 번호 입력 시스템이 제안되기도 했었다[8]. 하지만 그 후에 급속안구운동(saccadic eye movement)을 이용한 주위환기(convert attention)와 지각적 집단화(perceptual grouping)를 통해 공격자가 정보를 유추해 낼 가능성이 높다는 연구결과[9]가 나오며 멀티 라운드 프로토콜을 이용한 PIN 번호 입력 시스템은 그 의미를 잃었다. 이 외에 비시각적 정보를 이용한 어깨 넘어 훔쳐보기가 시행되었는데, 이것은 스마트폰의 가속도계의 진동을 감지하여 사용자의 비밀번호를 유추해 내는 방법이다[10]. 하지만 이 방법은 공격자가 사용자 스마트폰의 정확한 모델을 알고 있을 때 가능한 방법이라는 제한이 있다. 최근에는 증강 현실을 이용한 랜덤 키보드가 제안[11]되기는 하였으나 이 또한 증강현실을 위한 AR안경이라는 특수 장비가 동원되어야 가능한 방법이라는 제한이 있다. 기존 연구들은 모두 사용자의 비밀번호를 알면 무력화되거나, 그렇지 않더라도 특수 장비를 추가로 구입해야 한다는 공통점이 있다.

최근 주변에서 활용되고 있는 사용자 보호 시스템으로는 더미 숫자배열 키패드를 사용하거나, 사용자의 비밀번호 길이 추가 및 특수문자 사용(인터넷 뱅킹의 경우)을 권장하는 것 등이 있지만 사용되는 장소가 공공장소라는 특성으로 인해 여전히 비밀번호 유출의 위험성은 줄어들지 않고 있다. 또한 비밀번호의 복잡성이 높아질수록 사용자의 불편함과 부담 또한 높아지고 있다.

본 논문에서는 장소의 공개성이라는 동일한 조건 하에서도 원타임 키패드(One-Time Keypad, OTK)를 사용하면 비밀번호 유출에 안전함을 보이고자 한다[12]. 또한, 기존에 사용되던 키패드 및 OTP (One-Time Password)와의 보안성을 비교 분석하고자 한다. 이는 장소나 금융기기 같이 바꾸기 어려운 물리적인 조건 대신 개인의 보안 시스템을 변경함으로 기존 키패드와 OTK 중 사용 키패드를 정하는 선택권과 낮은 기회비용을 사용자에게 제공할 수 있다는 장점이 있다. OTK는 별도의 통신 채널 없이 기존의 ATM 기기의 소프트웨어 부분만 변경하면 사용 가능한 것으로 사용자가 OTK 선택 시 은행 서버를 통해 사용자의 단말기로 OTK를 송신하는 방식으로 운영된다. 이를 통해 일정 주기마다 비밀번호를 변경하며 그것을 기억해야 했던 사용자의 불편함을 해소할 수 있다.

II. 원타임 키패드

거래 시 추가인증 수단으로 많이 사용되는 것 중 하나는 OTP(One-Time Password)이다([13],[14],[15]). OTP는 거래 시마다 한 번만 사용할 수 있는 비밀번호를 매번 생성하여 인증함으로써 보다 안전한 전자거래가 가능하도록 하는 인증기술로 흔히 은행에서 발급받는 OTP 토큰을 통한 인증이 이에 속한다. OTP는 생성하는 방식에 따라 시도-응답방식, 시간동기화방식, 이벤트동기화방식, 시간-이벤트 혼합방식으로 나뉜다. 여기서는 국내 인터넷 뱅킹에 주로 사용되는 시간동기화 방식 OTP만 언급하도록 하겠다. 시간동기화 방식이란 보통 1분에 한 번씩 OTP를 생성하고 이를 인터넷뱅킹 화면에 입력한 후 금융회사 또는 OTP 통합인증센터를 통해 OTP의 유효성을 인증하는 방식이다. OTP는 불규칙적인 난수 규칙에 의해 일회용 비밀번호를 생성하기 때문에 공격자가 비밀번호를 획득하기 어렵다는 장점이 있으나, 일단 비밀번호를 획득한 후에는 일정 시간 안에

공격이 가능하다는 단점이 있다([16],[17]).

여기서 살펴볼 OTK(One-Time Keypad)는 이러한 공격에도 안전한 비밀번호 입력 스킴으로 제안될 수 있다. OTK는 크게 키패드 입력 장치와 단말기로 구성되어 있다. 키패드 입력 장치는 식별표지가 삭제된 널(null) 키패드를 입력창에 출력하여 사용자로부터 보안키를 입력받는 키패드 입력부와 랜덤 키패드를 생성하는 키패드 생성부로 나누어져 있다. 사용자가 등록한 단말기는 키패드 생성부에 의해 생성된 랜덤 키패드와 시간 동기화된 랜덤 키패드를 생성하여 디스플레이모듈을 통해 출력한다. 이렇게 출력된 랜덤 키패드를 확인한 사용자는 Fig.1.과 같이 입력장치에서 출력한 널 키패드에 비밀번호를 입력하여 사용자 인증을 한다. 이것은 기존의 사용자 인증 방식과 차별화된 방식으로 OTK는 다음과 같은 특징을 가졌다.

1. 키패드 입력장치와 단말기에 공유된 공유키 및 생성시각에 따라 생성되는 동기화키를 이용하여 배열키를 불규칙적인 난수 규칙에 의해 생성하고, 이 배열키를 키패드에 매칭한 후 서로 동기화시켜 랜덤 키패드를 생성한다.
2. 키패드 입력장치의 키패드는 널(null) 키패드로 출력된다.
3. OTK를 이용하여 비밀번호를 입력하려고 할 때 키패드 생성부에 의해 생성된 랜덤 키패드와 시간 동기화된 랜덤 키패드가 사용자의 단말기로 출력된다.

OTK는 현금자동입출기기, 인터넷 뱅킹, 도어락 등에 사용될 수 있는데 이 때 각 경우에 사용되는 키패드를 입력장치, 사용자의 스마트폰을 키패드 확인용 단말기라 할 수 있다. 즉, 키패드 생성부에서 생성한 랜덤 키패드와 시간 동기화된 랜덤 키패드를 스마트폰에서 확인한 후 널(null)키패드에 비밀번호를 입력하여 사용자 인증을 하는 것이다. 예를 들어, 현금자동입출기기에서 비밀번호가 2988인 사용자가 OTK로 비밀번호

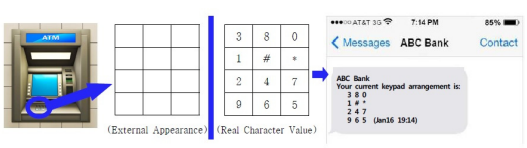


Fig. 1. OTK(One-Time Keypad)

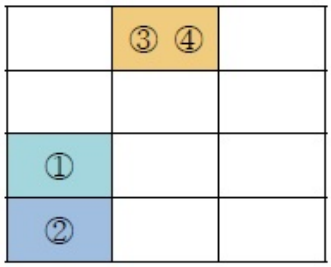


Fig. 2. Inserting password 2988 on null keypad

입력할 것을 선택한다고 하자. 그러면 Fig.1에서와 같이 사용자가 등록한 단말기로 랜덤 키패드가 시간 동기화 되어 출력되고 이를 확인한 사용자는 Fig.2.와 같이 현금자동입출기기의 널 키패드에 해당 번호가 있는 위치를 클릭하여 사용자 인증을 한다. 이 경우 현금자동입출기기의 키패드에 대해 어깨 넘어 훔쳐보기 공격을 시도하더라도 키패드가 공백 상태로 출력되기 때문에 공격에 안전함을 알 수 있다.

III. OTK의 보안성

3.1 4자리 비밀번호

현재 현금자동입출기기에서는 숫자로만 이루어진 4자리 비밀번호로 사용자 인증을 하고 있다. 키패드는 4x3 배열로 출력되며 0에서 9까지의 숫자와 *, #의 두 특수문자로 이루어져 있다. 여기서는 4자리 숫자 비밀번호의 모든 유형을 살펴보고 OTK 키패드와 기존의 키패드 사용에 어떤 차이가 있는지 IV에서 알아보고자 한다.

숫자 4자리 비밀번호는 모두 5가지 유형으로 나뉠 수 있다. 반복되는 숫자의 개수에 따라 반복되는 숫자가 없는 경우는 (A,B,C,D)로, 숫자 하나가 두 번 반복되는 경우는 (A,A,B,C)로, 숫자 두 개가 두 번

Table 1. Number of possible 4-digit passwords for each type

password type	number of possible passwords
(A,B,C,D)	${}_{10}P_4 = 5040$
(A,A,B,C)	$({}_{10}C_3)(3)(4!/2!) = 4320$
(A,A,A,B)	$({}_{10}C_2)(2)(4!/3!) = 360$
(A,A,B,B)	$({}_{10}C_2)(4!/(2!2!)) = 270$
(A,A,A,A)	${}_{10}C_1 = 10$
Total	$10^4 = 10000$

씩 반복되는 경우는 (A,A,B,B)로, 숫자 하나가 세 번 반복되는 경우는 (A,A,A,B)로, 숫자 하나가 네 번 반복되는 경우는 (A,A,A,A)로 표시한다. 각 유형별로 모든 순서를 고려하여 가능한 비밀번호의 개수를 계산하여 정리해보면 Table 1.과 같다.

이렇게 비밀번호를 유형별로 나누어 살펴보는 것이 중요한 이유는 현금자동입출기기의 키패드가 공백 상태로 표시된다 하더라도 비밀번호 입력 시 반복되는 숫자 유무사실은 노출되기 때문이다. Table 2.에는 각 유형의 비밀번호를 널 키패드에 입력할 때 가능한 입력위치의 개수를 정리하였다.

이는 또한 비밀번호의 유형이 알려져 있을 때 공격자가 시도할 수 있는 유형별 전수조사 횟수로 해석할 수 있다. (A,B,C,D) 유형의 비밀번호는 OTK를 통해 입력할 때 기존 키패드보다 2.34배 더 많은 경우의 수가 존재한다. 다른 유형의 경우는 각각 기존 키패드보다 (A,A,B,C)는 1.75배, (A,A,A,B)는 1.46배, (A,A,B,B)는 1.46배, (A,A,A,A)는 1.2배 더 많은 경우의 수가 존재한다. 유형을 고려하지 않을 때 OTK를 통한 키패드 입력의 경우의 수는 기존 키패드에 비해 2배 이상 많이 존재함을 알 수 있다.

이를 통해 OTK가 기존 키패드에 비해 전수조사 공격에 더 안전하다고 할 수 있다.

Table 2. Number of possible keypad positions for 4-digit password of each type

password type	number of possible keypad positions
(A,B,C,D)	${}_{12}P_4=11880$
(A,A,B,C)	$({}_{12}C_3)(3)(4!/2!)=7920$
(A,A,A,B)	$({}_{12}C_2)(2)(4!/3!)=528$
(A,A,B,B)	$({}_{12}C_2)(4!/(2!)(2!))=396$
(A,A,A,A)	${}_{12}C_1=12$
Total	$12^4=20736$

3.2 6자리 비밀번호

현재 사용 중인 4자리 비밀번호는 정보유출의 위험성이 커서 이에 대한 대책이 필요한 실정이다. 이에 유럽의 많은 나라는 이미 통장, 카드 등의 비밀번호를 6자리로 바꿔 사용하고 있고 인터넷 뱅킹에서 사용되는 OTP도 6자리 랜덤 숫자를 사용하고 있다. 따라서 OTK의 6자리 비밀번호에 대한 보안성 분석은 4자리 비밀번호가 6자리로 바뀌거나 OTP를 대체하는 경우에 적용될 수 있다.

통장이나 카드의 경우 비밀번호가 6자리로 늘어나면 보안성이 좋아지는 반면 기존보다 기억해야 하는 정보의 양이 많아져 사용자의 불편함도 증가한다는 단점이 있다. 이 뿐 아니라 주기적으로 비밀번호를 변경해야 하는 경우, 사용자의 비밀번호에 대한 부담은 가중된다. 이 때, 사용자의 역할을 OTK 인증 시스템이 대신한다면 사용자가 비밀번호를 주기적으로 변경해야 하는 부담이 줄 수 있다.

OTK에서 비밀번호 입력 위치의 가짓수를 알아보기 위해 각 유형별 비밀번호의 개수를 정리해보면 Table 3.과 같이 나온다는 것을 알 수 있다. 0부터 9까지의 숫자로 이루어진 6자리 비밀번호는 반복되는 숫자의 개수에 따라 총 11개의 유형으로 나눌 수 있다.

여기서 주목할 부분은 두 번 반복되는 수가 하나인 (A,A,B,C,D,E) 유형과 두 번 반복되는 수가 두 개인 (A,A,B,B,C,D) 유형이 비밀번호가 반복되는 수가 없는 (A,B,C,D,E,F) 유형의 비밀번호보다 각각 3배, 1.5배 더 많다는 것이다. 이것은 4자리 비밀번호에서 반복되는 수가 없는 (A,B,C,D) 유형의 비밀번호가 가장 많았던 것과 비교되는 결과이다. 6자리 비밀번호 사용자에게 위 두 유형의 비밀번호를 권장하는 것은 개인정보의 보안성을 높이는 방법 중 하

Table 3. Number of possible 6-digit passwords for each type

password type	number of possible passwords
(A,B,C,D,E,F)	${}_{10}P_6=151200$
(A,A,B,C,D,E)	$({}_{10}C_5)(5)(6!/2!)=453600$
(A,A,A,B,C,D)	$({}_{10}C_4)(4)(6!/3!)=100800$
(A,A,A,A,B,C)	$({}_{10}C_3)(3)(6!/4!)=10800$
(A,A,B,B,C,D)	$({}_{10}C_4)({}_4C_2)(6!/(2!2!))=226800$
(A,A,A,B,B,C)	$({}_{10}C_3)(2)({}_3C_2)(6!/(3!2!))=43200$
(A,A,B,B,C,C)	$({}_{10}C_3)(6!/(2!2!2!))=10800$
(A,A,A,A,A,B)	$({}_{10}C_2)(2)(6!/5!)=540$
(A,A,A,A,B,B)	$({}_{10}C_2)(2)(6!/4!2!)=1350$
(A,A,A,B,B,B)	$({}_{10}C_2)(2)(6!/3!3!)=900$
(A,A,A,A,A,A)	${}_{10}C_1=10$
Total	$10^6=1000000$

Table 4. Number of possible keypad positions for 6-digit password of each type

password type	number of possible keypad positions
(A,B,C,D,E,F)	${}_{12}P_6=665280$
(A,A,B,C,D,E)	$({}_{12}C_5)(5)(6!/2!)=1425600$
(A,A,A,B,C,D)	$({}_{12}C_4)(4)(6!/3!)=237600$
(A,A,A,A,B,C)	$({}_{12}C_3)(3)(6!/4!)=19800$
(A,A,B,B,C,D)	$({}_{12}C_4)({}_4C_2)(6!/(2!2!))=534600$
(A,A,A,B,B,C)	$({}_{12}C_3)(2)({}_3C_2)(6!/(3!2!))=79200$
(A,A,B,B,C,C)	$({}_{12}C_3)(6!/(2!2!2!))=19800$
(A,A,A,A,A,B)	$({}_{12}C_2)(2)(6!/5!)=792$
(A,A,A,A,B,B)	$({}_{12}C_2)(2)(6!/4!2!)=1980$
(A,A,A,B,B,B)	$({}_{12}C_2)(2)(6!/3!3!)=1320$
(A,A,A,A,A,A)	${}_{12}C_1=12$
Total	$12^6=2985984$

나가 될 수 있다.

Table 3.의 각 유형별 비밀번호를 OTK에 입력하는 위치의 가짓수는 Table 4.와 같다. OTK에서는 (A,B,C,D,E,F) 유형의 비밀번호가 기존의 키패드보다 4.4배 더 많은 입력 방법을 가지며, (A,A,B,C,D,E)는 3.14배, (A,A,A,B,C,D)는 2.36배, (A,A,A,A,B,C)는 1.83배, (A,A,B,B,C,D) 유형은 2.36배, (A,A,A,B,B,C)는 1.83배, (A,A,B,B,C,C)는 1.83배, (A,A,A,A,A,B) 1.47배, (A,A,A,A,B,B)는 1.47배, (A,A,A,B,B,B)는 1.47배, (A,A,A,A,A,A)는 1.2배 더 많은 입력 방법을 가진다.

유형을 고려하지 않는다면 OTK를 통한 키패드 입력의 경우의 수는 기존 키패드에 비해 약 3배 많이 존재한다. 이를 통해 OTK가 기존 키패드에 비해 전수조사 공격에 더 안전하다고 할 수 있다.

IV. OTK vs non-OTK

본 장에서는 OTK와 non-OTK 시스템의 보안성을 비교해 보기로 한다. 여기서 non-OTK라 함은 기존의 현금자동입출기기의 고정 키패드와 OTP를 뜻한다. 기존에 사용되던 키패드 및 OTP의 안전성과 OTK의 안전성을 비교해 보고 이들의 보안성에 대해 논하겠다.

4.1 단기 기억량

Alvarez와 George의 논문[18]에서 보면

$$C = I \times N$$

으로 총 정보량(C)은 각 아이템의 정보량(I)과 아이템의 개수(N)의 곱이다. 이 때 단기 기억량을 C라 하고 이 값이 고정되어 있다는 가정 하에 위 식을 다시 살펴보면, I와 N은 반비례 관계로 한 아이템 당 정보량이 많은 경우에는 기억할 수 있는 아이템의 수가 적어지고, 이와 반대로 아이템 당 정보량이 적은 경우에는 기억할 수 있는 아이템의 개수가 늘어난다는 것을 알 수 있다. 결과적으로 아이템의 복잡도와 기억할 수 있는 아이템의 수 사이에는 trade-off가 존재한다는 것이다. 또한 이 논문에서 밝히고 있는 것은 아무리 아이템의 정보량이 적다고 하더라도 기억할 수 있는 아이템의 개수가 무한히 늘어나는 것이 아니라 적당한 상계가 존재하여 그 이상은 기억하기 힘든 것이 보편적인 경우라는 것이다. 이 때 상계로 얻은 결과는 4~5로 한 번에 외울 수 있는 아이템의 개수는 많아야 4~5개로 한정되어 있음을 알 수 있다.

이 결과로부터 기존의 고정 키패드 상에서 4자리 비밀번호를 입력할 때 어깨 넘어 훔쳐보기 공격이 매우 성공적일 수 있다는 것과, 반대로 OTK의 경우에는 같은 공격으로 비밀번호를 알아내기란 거의 불가능 하다는 것을 알 수 있다. 즉, 단말기에서 출력되는 랜덤 키패드를 보고 12자리 숫자 배열을 외워 널 키패드에 입력하는 비밀번호의 위치를 통해 비밀번호를 알아내는 것은 거의 불가능하다는 것이다.

4.2 키패드의 수평각

4.1절에서 기존에 사용되는 고정 키패드와 OTK를 비교하였다면, 이 절에서는 현재 사용되는 키패드 중 OTK와 가장 유사한 경우인 현금자동입출기기에 랜덤 키패드를 직접 보여주고 비밀번호를 입력하는 경우와 단말기에서 랜덤 키패드를 출력한 후 널 키패드에 비밀번호를 입력하는 OTK의 경우를 비교해 보고자 한다.

사용자가 비밀번호를 입력하는 모습이 촬영되는 경우에 대해 현금자동입출기기에 랜덤 키패드를 직접 보여주는 시스템과 등록된 단말기에서 랜덤 키패드를 출력하고 널 키패드를 통해 비밀번호를 입력하는

OTK를 비교해 보면, Fig.3.에서 볼 수 있듯이 두 경우에 허용된 시야범위가 현저히 차이나는 것을 알 수 있다.

Fig.3.은 현금자동입출기기 키패드의 시야 범위를 수평각으로 나타낸 것이다. β=0을 기준으로 좌우로 45°(315°≤β≤45°)는 사용자가 몸으로 가리고 있는 공간이고 90°≤β≤270°은 칸막이로 막혀있는 범위이다. 그 외에 45°≤β≤90°와 270°≤β≤315°가 어깨 넘어 훔쳐보기 공격이 가능한 범위이다. 즉, 기존의 키패드 사용 시스템은 사용자의 몸으로 가리지 못하는 공간이 약 90° 정도 존재한다고 할 수 있다. 이는 기존 키패드 시스템이 랜덤 키패드를 사용하더라도 어깨 넘어 훔쳐보기 같은 비기술적 공격들은 근본적으로 차단하지 못한다는 것을 의미한다.

이에 비해 OTK는 단말기에서 출력하는 랜덤 키패드를 확인할 때 사용자가 단말기를 수직으로 세워 몸으로 적절히 감추며 확인할 수 있고 공격자는 현금자동입출기기와 같은 시야를 확보할 수 없다. 이 때 사용자의 주관적인 사용 패턴으로 인해 모든 경우에 동일한 보안성을 제공한다고 할 수는 없으나 입력 키패드와 키패드 표시창이 분리되어 있어 OTK가 물리적으로 제공하는 보안성은 기본적으로 제공된다고 할 수 있다.

스마트 폰에서 비밀번호 입력 시 어깨 넘어 훔쳐보기 공격이 이루어진다는 연구결과[6]가 나와 있으나 이는 본 장에서 다루는 상황과 동일하지 않은 경우임을 언급하고자 한다. 스마트 폰에서 비밀번호를 입력할 때는 스마트폰을 수직으로 세운 상태에서 입력하기 어렵고 또한 팔을 뻗어 입력해야 하므로 사용자의 몸에서 어느 정도 떨어진 위치에서 진행되는 반면, OTK는 스마트 폰에서 출력하는 키패드만 확인하면 되기 때문에 스마트 폰을 수직으로 세워 키패드 노출을 차단할 수 있다. 이는 어깨 넘어 훔쳐보기 공격, 카메라 촬영 등과 같은 사회 공학적인 공격을 근원적으로 차단할 수 있음을 의미한다.

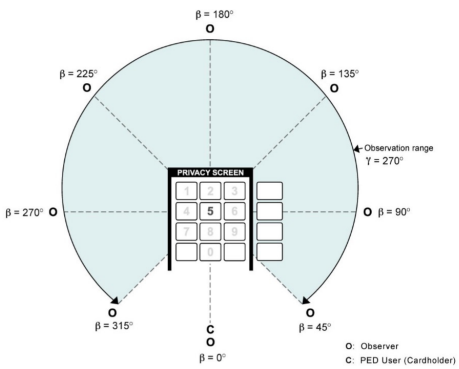
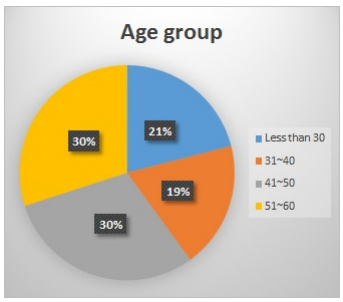


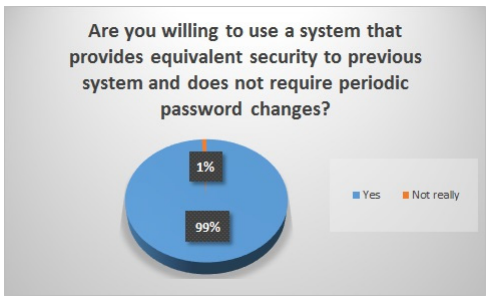
Fig. 3. Horizontal angle of keypad[19]

4.3 OTK 구현 및 사용자 사용 사례 연구

본 절에서는 OTK와 기존의 키패드를 스마트폰에 구현하여 사용자들의 사용 사례를 분석해보도록 한다. 타겟 보드로는 갤럭시탭 S2와 G Pro2을 선택하였다. 갤럭시탭 S2에는 가상 현금자동입출기기를 구현하는 애플리케이션을 실행하고 이와 동기화되어 실행되는 OTK 애플리케이션은 G Pro2에 실행하여 사용자들에게 기존 키패드와 OTK 두 가지를 모두 경험하도록 한 후 문항에 답하도록 하였다.

사용자는 모두 100명으로 연령대는 30대 미만부터 60세까지 다양한 연령대를 대상으로 사용 사례





조사를 실시하였다. 실험에 참가한 사용자 중 비밀번호를 잊어버린 경험이 있는지에 대해 78%가 그렇다고 대답하였고 한 개의 비밀번호를 변경할 필요 없이 사용해도 안전하다면 사용할 의향이 있는지에 대한 질문에는 99%가 그렇다고 대답하여 주기적으로 바꿔야 하는 비밀번호에 대한 사용자의 부담이 크다는 것을 확인할 수 있었다.

사용자들에게 가상 현금자동입출기기 화면(Fig. 4.)에서 예금출금을 선택하도록 한 후 우선 기존 키패드 화면(Fig. 5.)에 비밀번호를 입력하도록 하고 입력 시간을 측정하였다.

그 다음 Fig. 5.의 왼쪽 하단에 있는 OTK 아이콘을 선택하여 비밀번호를 입력하도록 하였다. 이 때 걸리는 시간은 키패드를 확인하는 순간부터 비밀번호를 입력하는 순간까지를 측정하였다. 두 경우 모두 비밀번호는 "1004"로 통일하였다.

사용자가 OTK를 선택하면 기존의 키패드 화면은 널키패드(Fig. 6.)로 화면이 바뀌고 사용자는 스마트폰의 OTK 랜덤 키패드(Fig.7.)를 보며 비밀번호를 입력해야 한다.

두 종류의 키패드에 비밀번호를 입력하는 시간을 통해 신속성을 측정해 보았다. 기존의 고정 키패드는 평균 2초가 나온 반면 OTK는 평균 4.19초로 기존

Fig. 4. Virtual ATM screen implemented on Galaxy Tab S2

Fig. 5. Fixed keypad

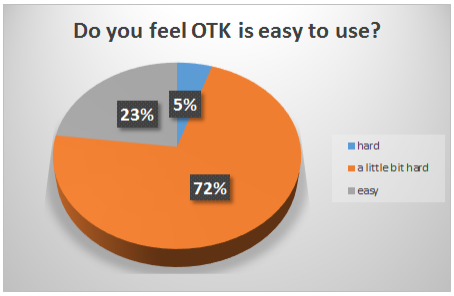
Fig. 6. OTK ATM screen

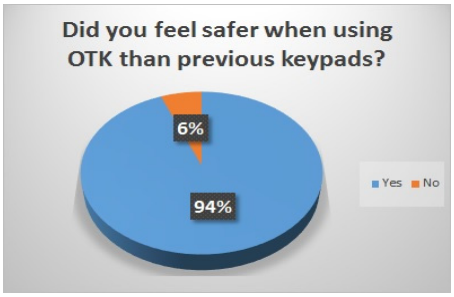
Fig. 7. OTK implemented on G Pro2

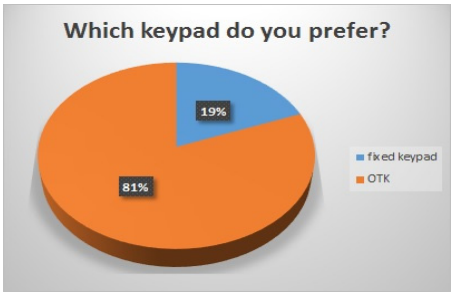
키패드보다 약 2배의 시간이 걸리는 것을 알 수 있었고, 실제로 사용자 중 73%는 기존 키패드보다 OTK 사용이 조금 더 불편하다고 응답하였다. 하지만 OTK 사용이 많이 불편하다고 답한 사용자는 5%에 불과하였고, OTK 사용이 기존 키패드보다 안전하다고 느끼는 사용자는 94%였다. OTK와 기존 키패드 중 어느 시스템을 선호하는지에 대한 질문에 81%가 OTK를 사용하고 싶다고 응답하였고 위 질문들을 통합해 보았을 때, OTK의 신속성은 기존 키패드에 비해 떨어지는 것이 사실이나 OTK가 제공하는 안전성을 함께 고려할 때 OTK의 신속성은 사용자가 수용할만한 범위 안에 있음을 알 수 있다.

4.4 OTK와 키패드 사이즈

공격자가 비밀번호의 자릿수 k만 알고 있는 경우 공격자가 비밀번호를 알아낼 확률은 non-OTK의 경우에 $1/10^k$ 이고 OTK의 경우에 $1/12^k$ 이다. 이때, 키패드의 사이즈를 늘리면 비밀번호를 알아낼 확







률은 더 줄어들게 된다. 비밀번호가 길어지면 보안성은 증가하겠지만 사용자의 불편함 또한 같이 증가함을 고려할 때 비밀번호는 기존의 4~6자리로 유지하고 키패드의 사이즈를 늘리면 사용자의 편의를 고려하며 보안성을 높일 수 있다. Table 5.는 OTK에서 비밀번호에 적용되는 키패드의 사이즈에 따라 가능한 모든 비밀번호 입력 위치의 개수를 보여주고 있다.

Table 5.에서 주목할 부분은 5자리 비밀번호를 4×4 키패드로 입력하는 비밀번호의 결과와 OTP에서 사용하는 6자리 숫자 집합의 크기가 근사하다는 것이다. 즉, 키패드 사이즈를 늘린 후 OTK를 이용하면 더 짧은 비밀번호로 OTP와 같은 보안성을 제공할 수 있다는 의미이다. 6자리 비밀번호의 경우, 기존의 4×3 키패드를 사용하면 OTP의 약 3배에 달하는 경우의 수가 존재하고 4×4 키패드를 사용하면 약 16.8배의 경우의 수가 존재함을 확인할 수 있다. 사용자 입장에서는 길이가 짧은 비밀번호가 선호

Table 5. Number of possible password positions on different keypad size

keypad size	password size		
	4-digit	5-digit	6-digit
4x3	20736	248832	2985984
4x4	65536	1048576	16777216
5x4	160000	3200000	64000000
5x5	390625	9765625	244140625

되는데, OTK는 non-OTK와 비교했을 때 4자리 비밀번호로 non-OTK의 6자리 비밀번호에 상응하는 보안성을 제공하고 같은 길이의 비밀번호에 대해서는 더 높은 보안성을 제공한다는 것을 알 수 있다.

4.5 비밀번호 유형의 공개

여기서는 공격자가 최소한 사용자의 비밀번호 유형은 알고 있다는 가정 하에 OTK와 non-OTK의 보안성을 비교해 보고자 한다.

아래와 같이 두 가지 경우로 나누어 생각해 볼 때 OTK와 non-OTK에 대해 Table 6.과 Table 7.과 같은 결과를 얻을 수 있다. 이 때, 두 경우 모두 랜덤 키패드와 랜덤 번호를 생성하는데 각각 1분의 간격이 있다고 가정한다.

- Case 1. 비밀번호를 정확히 알 때
- Case 2. 비밀번호 유형만 알 때

Case 1의 경우 4자리와 6자리에 대한 비밀번호가 모두 알려져 있다 하더라도 기존의 키패드나 OTP가 비밀번호를 알아낼 확률이 1인 것과 달리 OTK는 사용자 인증에 성공할 확률이 1/(가능한 비밀번호 입력 위치의 수)이다. 이는 OTK가 비밀번호 외에

Table 6. Probability of (4-digit) password leakage for each type

Password Type		Ordinary and OTP	OTK
(A,B,C,D)	Case 1	1	$\frac{1}{11880}$
	Case 2	$\frac{1}{5040-(n-1)}, n \le 5040$	$\frac{1}{11880-(n-1)}, n \le 11880$
(A,A,B,C)	Case 1	1	$\frac{1}{7920}$
	Case 2	$\frac{1}{4320-(n-1)}, n \le 4320$	$\frac{1}{7920-(n-1)}, n \le 7920$
(A,A,A,B)	Case 1	1	$\frac{1}{528}$
	Case 2	$\frac{1}{360-(n-1)}, n \le 360$	$\frac{1}{528-(n-1)}, n \le 528$
(A,A,B,B)	Case 1	1	$\frac{1}{396}$
	Case 2	$\frac{1}{270-(n-1)}, n \le 270$	$\frac{1}{396-(n-1)}, n \le 396$
(A,A,A,A)	Case 1	1	$\frac{1}{12}$
	Case 2	$\frac{1}{10-(n-1)}, n \le 10$	$\frac{1}{12-(n-1)}, n \le 12$

Table 7. Probability of (6-digit) password leakage for each type

Password Type		ordinary and OTP	OTK
(A,B,C,D,E,F)	Case 1	1	$\frac{1}{665280}$
	Case 2	$\frac{1}{151200-(n-1)}, n \le 151200$	$\frac{1}{665280-(n-1)}, n \le 665280$
(A,A,B,C,D,E)	Case 1	1	$\frac{1}{142560}$
	Case 2	$\frac{1}{453600-(n-1)}, n \le 453600$	$\frac{1}{1425600-(n-1)}, n \le 1425600$
(A,A,A,B,C,D)	Case 1	1	$\frac{1}{1237600}$
	Case 2	$\frac{1}{100800-(n-1)}, n \le 100800$	$\frac{1}{1237600-(n-1)}, n \le 1237600$
(A,A,A,A,B,C)	Case 1	1	$\frac{1}{19800}$
	Case 2	$\frac{1}{10800-(n-1)}, n \le 10800$	$\frac{1}{19800-(n-1)}, n \le 19800$
(A,A,B,B,C,D)	Case 1	1	$\frac{1}{534600}$
	Case 2	$\frac{1}{226800-(n-1)}, n \le 226800$	$\frac{1}{534600-(n-1)}, n \le 534600$
(A,A,A,B,B,C)	Case 1	1	$\frac{1}{79200}$
	Case 2	$\frac{1}{43200-(n-1)}, n \le 43200$	$\frac{1}{79200-(n-1)}, n \le 79200$
(A,A,B,B,C,C)	Case 1	1	$\frac{1}{19800}$
	Case 2	$\frac{1}{10800-(n-1)}, n \le 10800$	$\frac{1}{19800-(n-1)}, n \le 19800$
(A,A,A,A,A,B)	Case 1	1	$\frac{1}{792}$
	Case 2	$\frac{1}{540-(n-1)}, n \le 540$	$\frac{1}{792-(n-1)}, n \le 792$
(A,A,A,A,B,B)	Case 1	1	1980
	Case 2	$\frac{1}{1350-(n-1)}, n \le 1350$	$\frac{1}{1980-(n-1)}, n \le 1980$
(A,A,A,B,B,B)	Case 1	1	1320
	Case 2	$\frac{1}{900-(n-1)}, n \le 900$	$\frac{1}{1320-(n-1)}, n \le 1320$
(A,A,A,A,A,A)	Case 1	1	12
	Case 2	$\frac{1}{10-(n-1)}, n \le 10$	$\frac{1}{12-(n-1)}, n \le 12$

단말기에서 출력한 랜덤 키패드에 대한 정보도 함께 요구하기 때문이다. OTK는 비밀번호가 알려진 경우라 할지라도 공격자가 비밀번호와 단말기를 동시에 얻지 못하는 한 비밀번호를 모르는 경우와 동일한 효과를 낸다는 것을 알 수 있다. OTK와 non-OTK 두 경우 모두 최대 시행 횟수를 시도한 후 사용자 인증에 성공하였다 가정하고 (A,B,C,D) 유형을 살펴보면 비밀번호에 대한 전수조사 과정 중에 변하는 확률은 Fig.8.과 같다.

여기서 x축은 시행횟수이고 y축은 시행횟수에 따른 사용자 인증에 성공할 확률값이다. Fig.8.에서 볼 수 있듯이 비밀번호의 유형에 대한 정보가 알려진

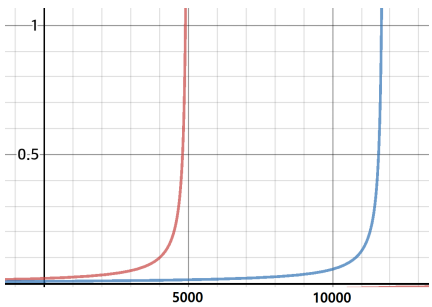


Fig. 8. Probability of (A,B,C,D) -type password leakage for OTK(blue) and non-OTK(red)

Table 8. Comparison of ordinary keypads, OTP, and OTK

	ordianry keypads	OTP	OTK
when password is disclosed	succeeds in user authenti-cation	succeeds in user authentica-tion	needs to know random keypad to succeed in user authentication
repetitive use of password	able to reuse password until user changes it	able to reuse password maximum of 1 minute	able to reuse password maximum of 1 minute
when device is lost	N/A	succeeds in user authentica-tion until user changes the device	needs to know password for user authentication

경우에라도 OTK의 확률 변화가 non-OTK 경우에 비해 매우 느리게 진행되어 1분의 인터벌 시간에 이루어질 수 있는 전수조사 공격에 non-OTP보다 저항성이 높음을 알 수 있다.

한 번 알아내면 사용자가 자신의 비밀번호가 노출되었다는 것을 감지하여 변경하기 전까지 반복 사용이 가능한 것에 비해 OTK는 사용자의 감지 여부와 상관없이 최대 1분 동안만 반복하여 사용 가능하다. 이를 비교하여 정리하면 Table 8.과 같다.

현재 사용되는 사용자 인증 방법에는 OTP나 고정 키패드처럼 번호를 통한 인증 외에도 다양한 방법이 존재한다. 이를 OTK와 비교 정리하면 Table 9.와 같다.

4.6 OTK의 변형

Table 6.과 Table 7.은 모두 랜덤 키패드/번호의 재생성까지 1분의 간격이 있다는 가정과 비밀번호 전체 혹은 그 유형만이 알려져 있다는 가정 하에 사용자 인증에 성공할 확률을 계산한 값이다. 이 때 가정으로 두었던 1분마다 재생성 되는 랜덤 키패드 시스템을 변형하여 비밀번호 한 자리마다 서로 다른 키패드를 사용하는 시스템을 사용한다면 앞에서 문제되었던 비밀번호 유형 노출 문제와 1분 동안 발생할 수도 있는 전수조사 공격에서 자유로울 수 있다.

6자리 비밀번호의 경우에 변형된 OTK에서 (A,A,B,C,D,E) 유형 비밀번호에 대한 전수조

Table 9. Comparison of authentication methods

Description	User & Password	NFC	SMS	ARS	Fingerprints	Iris	Face	OTP	OTK
Method	Intelligence	Possession	Possession	Possession	Biometric	Biometric	Biometric	Possession	Intelligence & Possession
How user's authentication is hacked?	Spy camera	Lost device	Lost device	Lost device	Copy	Copy	Copy	Lost device	Copy & Spy camera
Safe or dangerous with hacked password?	Dangerous	N/A	N/A	N/A	Dangerous	Dangerous	Dangerous	N/A	**Safe**
Safe or dangerous with hacked device?	N/A	Dangerous	Dangerous	Dangerous	N/A	N/A	N/A	Dangerous	**Safe**
Is user's authentication changeable?	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	**Yes**	**Yes**
Can be used at the unconscious (sleeping, etc)?	**No**	Yes	Yes	Yes	Yes	Yes	Yes	Yes	**No**
Usablity (User friendly)	**High**	Low	Average	Average	Low	Low	Low	Average	Low
Economic efficiency	**High**	Low	Average	Average	Low	Low	Low	Low	Low
Requirement for user	Change regularly	Not to be lost	Not to be lost	Not to be lost	Not to be copied	Not to be copied	Not to be copied	Not to be lost	Pratice

사 횟수는 1,425,600에서 12^6 으로 늘어나 약 2배가 됨을 알 수 있다. 이 유형은 6자리 비밀번호 중 가장 승수가 작은 유형이고, (A,A,A,A,A,A) 유형의 경우에는 변형 전 OTK 경우보다 12^5(=248,832)배가 되어 승수가 가장 큰 유형이라 할 수 있다. 즉, 변형된 OTK에서는 모든 유형에 대해 각각 12^6의 시행 횟수를 제공하기 때문에, 결과적으로 유형의 구분을 없애고 어깨 넘어 공격으로 유출 가능성이 있던 비밀번호 유형에 대한 정보 유출을 막을 수 있다. 또한 키패드 생성에 걸리던 1분의 시간을 없앰으로 기존에 가능했던 전수조사 공격으로부터 자유로워질 수 있다.

V. Conclusion

본 연구에서는 기존 키패드 사용에서 문제되던 어깨 넘어 훔쳐보기와 같은 사회공학적 공격에 대해 저항성을 가진 OTK 시스템에 대한 보안성을 비교·분석해 보았다. 사용자 사례 분석결과 OTK는 사용자가 OTK 표시장치에서 비밀번호 위치를 기억하며 현금자동입출기기에 정확하게 입력해야 하는 어려움이 있었다. 또한 키패드 사용시 추가 장비인 단말기를 이용해야 한다는 번거로움도 있었다. 하지만 이러한 번거로움에도 불구하고 81%의 사용자가 OTK 사용을 선호하였다. 이는 랜덤 키패드를 기억하는 방법이 기존 키패드 사용법보다 다소 어렵기는 하였으나 사용자가 수용할 수 있는 범위 내였기 때문이고, 추가 장비인 단말기는 사용자의 스마트폰을 활용하는 시스템이었기 때문이다. 기존 다른 연구에서 제안된 시스템과 달리 OTK는 사용자나 시스템 제공자에게 발생하는 추가비용이 없다. 또한, 매 주기마다 비밀번호를 변경하거나 복잡한 비밀번호를 사용해야 했던 사용자의 불편함을 고려하여 비밀번호를 변경하지 않고 사용하더라도 4자리/6자리 비밀번호의 경우 고정 키패드 시스템보다 각각 평균 2배, 3배 이상의 보안성을 확보할 수 있었다. 또한 non-OTK(기존에 사용하던 고정 키패드 시스템과 OTP)에서의 취약점을 개선할 수 있음을 수치적으로 분석하였다. 우선, 전수조사 공격에 대한 저항성과 키패드 사이즈에는 양의 상관관계가 있음을 수치적인 결과를 통해 알게 되었다. 그리고 비밀번호가 모두 노출된 경우에 사용자 인증에 성공할 확률이 1이었던 기존의 non-OTK 시스템과 달리 OTK에서는 비밀번호가 모두 노출된 경우에도 랜덤 키패드에 대한 정보 없으면 비밀번호에 대한 정보가 유명무실해짐을 확인하였다. OTK와 non-OTK의 보안성을 여러 각도에서 비교·분석하여 같은 조건 하에서도 OTK의 보안성이 평균적으로 2배 정도 높다는 결과를 얻었고, 물리적 조건을 바꾸거나 기존 시스템을 변경하는데 시간과 비용을 소모하는 대신 OTK를 사용하는 것이 사용자의 만족도와 보안성을 모두 높일 수 있음을 확인하였다.

References

[1] The Bank of Korea, "Use of internet banking services during Q3 2016", Nov. 2016.

[2] Korea Internet and Security Agency, "2016 Survey on information security (individual) executive summary", Jan. 2017.

[3] Financial Security Agency, "Guide to financial applications of cryptographic techniques", Nov. 2014.

[4] 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 & Cryptology, 24(6), pp. 1159-1174, Dec. 2014 .

[5] H. Kim, H. Kim, Y. Lee, T. Park, and H. Seo, "Realization of virtual security keypad against shoulder surfing attack," Journal of The Korea Institute of Information Security & Cryptology, 23(6), pp. 21-29, Dec. 2013.

[6] H. Seo and H. Kim, "Design of Security Keypad Against Key Stroke Inference Attack", Journal of The Korea Institute of Information Security & Cryptology, 26(1), pp. 41-47, Feb. 2016.

[7] I. Kim, "Keypad against brute force attacks on smartphones," IET Information Security, vol. 6, no. 2, pp. 71-76, Jun. 2012.

[8] V. Roth, K. Richter, and R. Freidinger, "PIN-entry method resilient against shoulder surfing," In Proceedings of the 11th ACM Conference on Computer and Communications Security pp. 236-245, Oct. 2004.

[9] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol.44, no.6, pp.716-727, Jun. 2014.

[10] P. Marquardt, A. Verma, H. Carter, and P. Traynor, "(sp) iphone: Decoding vibrations from nearby keyboards using mobile phone accelerometers," Proceedings of the 18th ACM Conference on Computer and Communications Security, pp. 551-562, Oct. 2011.

[11] A. Maiti, M. Jadliwala, and C. Weber, "Preventing shoulder surfing using randomized augmented reality keyboards," Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 630-635, Mar. 2017.

[12] S. Choi, "Inputting system and method for security key using one time keypad", Korean Patent, 10-1629495, Jan. 2017.

[13] K. Kim, "A study on user authentication based on One-Time Password", Journal of The Korea Institute of Information Security & Cryptology, 17(3), pp. 26-31, Jun. 2007.

[14] K. Kim "One-Time Password (OTP) integrated authentication service framework", TTA Journal, 153(5), pp. 56-61, May 2014.

[15] C. Xiao-rong, F. Qi-yuan, D. Chao, and Z. Ming-quan, "Research and realization of authentication technique based on OTP and Kerberos," In Proceedings of Eighth International Conference on High-Performance Computing in Asia-Pacific Region, pp. 409, Jul. 2005.

[16] Foo Kune, Denis, and Yongdae Kim, "Timing attacks on pin input devices," Proceedings of the 17th ACM Conference on Computer and Communications security, pp. 678-680, Oct. 2010.

[17] C. Mulliner, R. Borgaonkar, P. Stewin, and J.P. Seifert, "SMS-based one-time passwords: attacks and defense," Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability

Assessment, Springer Berlin Heidelberg, pp. 150-159, Jul. 2013.
〔18〕 G.A. Alvarez and P. Cavanagh, "The capacity of visual short-term memory is set both by visual information load and by number of objects," Psychological Science vol.15, no.2, pp. 106-111, Feb. 2004.
〔19〕 PCI Security Standards Council, "Information supplement: ATM security guideline", Jan. 2013.

〈저자소개〉

김 종 락 (Jon-Lark Kim) 정회원
1993년 2월: POSTECH 수학과 졸업
1997년 2월: 서울대학교 수학과 석사
2002년 5월: University of Illinois at Chicago 수학과 박사
2005년 8월: University of Nebraska at Lincoln 수학과 연구조교수
2012년 8월: University of Louisville 수학과 조교수, 부교수
2012년 9월~현재: 서강대학교 수학과 교수
〈관심분야〉 부호론, 암호론, 산업수학, 인공지능

이 나 리 (Nari Lee) 학생회원
2009년 2월: 서강대학교 수학과 졸업
2011년 2월: 서강대학교 수학과 석사
2011년 9월~현재: 서강대학교 수학과 박사과정
〈관심분야〉 부호론, 암호론

노 영 건 (Young Gun Roe) 학생회원
1996년 9월: Imperial College London 수학과 졸업
1997년 9월: Imperial College London 수학과 석사
2015년 9월~현재: 서강대학교 수학과 박사과정
〈관심분야〉 부호론, 암호론

Lucky Erap Galvez 학생회원
2007년 4월: University of the Philippines 수학과 졸업
2011년 10월: University of the Philippines 수학과 석사
2015년 9월~현재: 서강대학교 수학과 박사과정
〈관심분야〉 부호론, 암호론