Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.1, Feb. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.1.41

입력 위치 유추 방지를 위한 보안 키패드의 설계*

서 화 정,† 김 호 원‡
부산대학교

Design of Security Keypad Against Key Stroke Inference Attack*

Hwajeong Seo,† Howon Kim‡
Pusan National University

요 약

Black hat USA 2014에서는 사용자가 스마트폰 혹은 스마트패드 상에서 비밀번호 입력 시 공격자가 구글 글라스를 이용하여 원거리에서 입력되는 비밀번호의 위치점을 유추해 내는 기술을 시연하였다. 본 논문에서는 동일한 입력값에 대해서도 상이한 위치점을 갖도록 설계한 키패드를 제안함으로써 구글 글라스와 같은 스마트 디바이스를 이용한 공격을 효과적으로 방어할 수 있는 방안에 대해 제시한다.

ABSTRACT

In Black hat USA 2014, a hacking method to infer the password entry of smartphone or smartpad with google glass in distance is presented. In this paper, we design the secure keypad to protect the key stroke inference attacks with google glass which has unique layout ensuring same input entry but different input value.

Keywords: Security Keypad, Input Location Prediction Attack

I. 서 론

블랙햇 USA 2014에서는 구글 글래스를 이용하여 3m 떨어진 거리에서 사용자가 터치스크린를 통해 비밀번호를 입력하는 모습을 촬영한 다음 사용자의 손동작을 분석하여 90%의 정확도로 비밀번호를 유추해내는 어깨너머 공격을 선보였다 [1]. 이를 방지하기 위해 화면상에 나타나는 키패드의 위치를 무작위로 변경하여 공격자가 사용자의 손끝이 향하는 위치점을 유추하더라도 정확한 키패드의 값을 확인하는 것이 불가능하게 하는 기법이 제안되고 있다. 해당 기법은 구글 글라스를 통한 유추공격에는 강인하지만 사용자의 입력 편이성이 저하되는 문제점을 가지고 있다. 따라서 구글 글라스에 의한 원거리 어깨너머 공격을 효과적으로 방어함과 동시에 사용자가 편하게 입력이 가능한 키패드 방어 기법에 대한 연구가 필요하다.

본 논문에서는 기존의 보안 키패드의 보안 취약점을 개선하는 위치점 유추 방지 키패드를 제안한다. 해당 키패드는 기존의 무작위로 배치하여 위치점을 방어하는 기법과 달리 사용자에게 최소한의 키패드 위치 배치 정보를 제공하여 편의성을 극대화시켰다. 이를 통해 사용자는 기존의 무작위 배치와 동일한 보안강도를 가지지만 입력 속도는 향상되는 보안키패드를 통해 보다 빠르고 안전하게 자신의 비밀번호를 스마트 장비 상에서 입력하는 것이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서는 입력정

Received(09. 10. 2015), Modified(12. 07. 2015), Accepted(12. 07. 2015)
* 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No.10043907, 개방형 고성능 표준 IoT 디바이스 및 지능형 SW 개발)과 산업통상자원부 우수기술연구센터(ATC)사업(10048537)과 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2015-H8501-15-1017)
† 주저자, hwajeong84@gmail.com
‡ 교신저자, howonkim@pusan.ac.kr (Corresponding author)

보 보호 관련 연구에 대해 살펴본다. 3장에서는 제안하는 키패드에 대해 제시하며 4장에서는 이에 대한 성능 평가를 한다. 마지막으로 5장에서는 본 논문의 결론을 내린다.

II. 입력지점에 대한 입력정보 보호 관련 연구

입력지점에 대한 입력정보 보호를 위해서는 정보 입력 시 키패드에 발생하는 물리적인 특징으로 키를 유추하는 키 로깅 공격을 방지해야 한다. 키 로깅 공격기법은 사용자의 PC 혹은 스마트폰 상에서 키보드의 키 입력을 추적하거나 기록하는 기법으로서, 소프트웨어, 하드웨어, 원격 RF 그리고 음향 분석 기반 기법 등이 있다 [2].

최근에는 웨어러블 디바이스인 구글 글라스의 등장으로 원거리에게 어깨너머 공격을 자동으로 수행하는 기법이 제안되었다 [1]. 해당 기법은 Deformable Part-based Model을 기반으로 한 물체 인식과 k-means clustering을 통해 사용자가 입력하는 값을 유추한다. 구글 글라스를 통한 어깨너머 공격을 효율적으로 대처하기 위해 키패드에 표기되는 문자를 무작위로 배열함으로써 키패드의 정보를 유추하는 것이 불가능하게 하는 기술이 제안되고 있다.

해당 기법은 키보드 레이아웃의 기본 틀은 만족하지만 키보드의 배치는 변경되도록 한다. 이는 사용자의 비밀번호 입력 시 상이한 비밀번호 레이아웃을 제공하여 레이아웃 정보를 이용한 공격이 불가능하도록 한다. 또 다른 방법은 레이아웃이 동적으로 변경되는 기법을 적용하여 공격을 효과적으로 방지하는 기법이다. 해당 두 기법 사용 시 어깨너머 공격을 효과적으로 방어할 수 있다. 하지만 사전에 알려진 레이아웃을 변경하여 새로운 형태로 키패드를 제작하는 경우 사용자는 해당 키보드를 사용하는 매 순간마다 레이아웃을 새롭게 익혀야 하는 문제점으로 인해 입력속도가 저하되는 문제점을 가진다.

III. 제안하는 보안 키보드

본 논문에서는 사용자의 위치점을 원거리에서 유추하여 사용자의 비밀번호를 알아내는 원거리 어깨너머 공격에 강인한 보안키보드를 제안한다. 제안하는 기법은 기존에 제안된 보안 키보드와 유사하게 키보드 상의 입력값을 무작위로 배치하여 보안성을 높인다. 하지만 스크린을 볼 수 있는 사용자에게 추가적인 키보드 배치 규칙을 제공하여 키보드 입력속도를 향상 시켰다. 이는 기존의 쿼티 키보드에 친숙한 사용자가 보안키보드 사용 시 기존의 키보드 배치 규칙을 일정 부분 유지함으로써 자신의 사전 지식을 보안 키보드와 조합하여 입력값의 위치를 쉽게 찾을 수 있는 기법이다.

원거리 어깨너머 공격에 대한 효과적으로 방어하기 위해서는 쿼티 키보드에 표기되는 입력값들을 무작위로 배치하면 가능하다. 하지만 이는 공개 표준화인 쿼티 키보드의 규칙을 무시함으로써 키보드의 배치와 위치 점에 대한 사용자의 사전지식을 제거하게 된다. 따라서 방어를 위한 방편으로 사용자 또한 기존 키보드 레이아웃이 주는 사용 편의성을 포기해야 한다는 문제점을 가진다. 본 논문에서는 기존의 보안 키보드에 비해 사용자의 편의성과 보안성을 동시에 향상시키는 기법에 대해 확인해 보도록 한다.

기존의 쿼티 키보드의 레이아웃은 크게 입력 창의 행과 열 그리고 인접 입력 값으로 생각해 볼 수 있다. 행에 대해 확인해 보면 “Q~P”문자열을 포함하는 1행, ″A~L”문자열을 포함하는 2행 그리고 ″Z~M”문자열을 포함하는 3행으로 구성된다. 열을 기준으로 살펴보면 1행에서는 “Q”가 가장 첫 번째 문자로 오게 되고 ″P”이 가장 마지막에 위치함을 확인할 수 있다. 2행에서는 “A”가 가장 첫 번째 문자로 배치되고 “L”이 가장 마지막에 위치함을 확인할 수 있다. 3행에서는 “Z”가 가장 첫 번째 문자로 오게 되고 “M”이 가장 마지막에 위치함을 확인할 수 있다. 마지막으로 확인해 볼 수 있는 정보로는 인접한 키들 간의 관계이다. 입력값 ″S”의 경우 좌측 위로는 “W”, 우측 위로는“E”, 동일한 열상의 좌측에는 “A”, 우측에는 “D”, 그리고 아래로는 “Z”를 확인할 수 있다. 이와같이 쿼티 키보드는 사용자에게 입력값 배치에 관한 사전 정보를 제공하여 쿼티 키보드에 대한 능숙도가 높아지는 경우 입력 속도를 향상 시킬 수 있다. 하지만 최근에 제안되는 어깨너머 공격의 경우 해당 사전 지식이 공격을 가능하게 하는 루트로 악용되는 사례가 늘고 있다. 이를 방어하기 위해 제안된 보안 키패드의 경우 쿼티키보드가 가지는 세 가지 사전 지식을 제거할 수 있지만 이는 사용자가 원하는 키보드를 쉽게 확인하는 것을 어렵게 하여 실용적인 적용이 어려운 문제가 있다.

본 논문에서는 기존의 보안 키보드의 문제점을 해

Table 1. Algorithm 1. Initializtion of keypad

Input: Random seed Output: Randomized keypad	
1	Random generation from seed
2	Divide the random by 4 (place them from 0 to 3) and make permutation
3	Align the row
4	Random generation from seed
5	Divide the random by 10 (place them from 0 to 9)
6	Set the offset with random
7	Correct column

결하기 위해 행과 열의 연관 정보 및 열에 대한 정보를 제거하지만 행을 기준으로 인접 입력값에 대한 정보는 유지하는 새로운 방식의 보안키보드를 제안한다. 이는 컴퓨터 구조상에서 메모리에 접근할 때 첫 번째 주소를 통해 전체 결과값을 유추하는 indirect 주소 방식을 보안 키보드에 적용한 기술이다. 제안하는 보안키보드는 숫자 입력까지 포함하여 총 36개의 입력값을 기준으로 확인해 보도록 한다.

기존의 쿼티 키보드는 총 4개의 열로 이루어지며 1행에는 10개, 2행에는 10개, 3행에는 9개 그리고 4행에는 7개의 입력값이 위치하도록 설계된다. 여기서 1행은 "1~0", 2행은 "Q~P", 3행은 "A~L", 4행은 "Z~M"으로 묶어서 값을 저장한다. 이를 통해 총 4개의 문자 배열(Input_Array)이 생성되게 된다. 첫 번째로 제안하는 보안키보드의 생성을 위해 난수 생성기에서는 4개의 인자에 대한 순열을 생성하게 된다. 이는 4개의 문자 배열의 출력 행의 위치를 결정하게 된다. 만약 난수 순열의 값이 〔4, 3, 1, 2〕 인 경우 "Z~M", "A~L", "1~0", "Q~P"으로 행이 선택되게 된다. 그리고 다시 난수값 (RNG)에 대한 10의 나머지 값을 계산한다. 이를 통해 "0~9"에 해당하는 값이 생성되며 이는 행의 시작점을 나타내는 행의 offset으로 설정되게 된다. 따라서 만약 해당 값이 4가 되고 열의 배치가 (4, 3, 1, 2)가 되는 경우의 예시는 Fig. 1.의 왼쪽 그림과 같다.

여기서 offset이 4가 되는 경우 앞의 offset에는 가장 하위의 값이 올라와서 채워지게 된다. 따라서 키보드의 구성은 rotation이 되어 전체 값을 나타낼 수 있도록 디자인되게 된다. 이는 rotation이 되지 않을 시 가장 상위 행과 가장 하위 행의 양 끝 입력값이 1/4의 확률로 유추가 가능하다는 문제점을 해

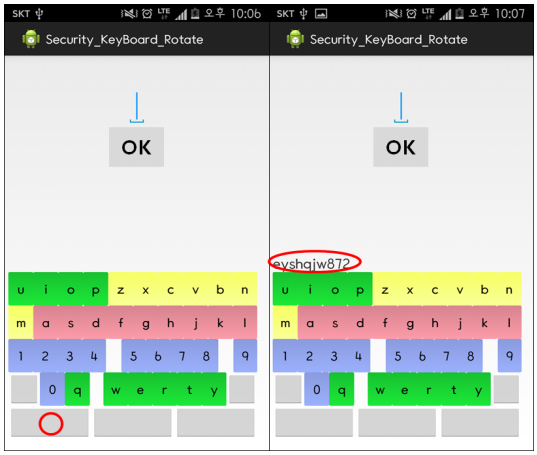

Fig. 1. Test environments of security keyboard (1/2)

결하기 위해 필요한 기술이다. 제안하는 키패드는 Table 1의 알고리즘 1을 통해 초기화되며 해당 알고리즘을 재사용하여 갱신된다. 전체적인 운영 기법은 Table 2의 알고리즘 2에 명시되어 있다.

제안한 기법을 사용하면 공격자는 사용자의 위치점을 찾는 것이 어렵다. 하지만 사용자의 비밀번호에 동일한 문자열이 포함된 경우 해당 비밀번호를 유추할 수 있다. 예를들어 비밀번호가"12341234"인 경우 해당 비밀번호는"1234"라는 동일한 문자에 대해 동일한 위치점을 가지게 되는 문제점을 가진다. 따라서 사용자의 비밀번호의 복잡도는 n^8(n의 문자의 수)에서 n^4로 줄어들게 된다. 따라서 이를 방지하기 위해서는 동일한 문자에 대해서도 서로 다른 위치점을 갖는 키패드에 대한 연구가 필요하다. 이를 방지하기 위해 두 번째 제안기법은 사전 지식인 양 옆의 인접 문자에 대한 정보는 제공하지만 위치점에 대한

Table 2. Algorithm 2. Operation of keypad

Input: Random seed Output: Randomized keypad	
1	Set the keypad with Algorithm 1
2	While(1)
3	if(Any key inputs)
4	if(Exit input)
5	Terminate the program
6	else
7	Set the keypad with Algorithm 1
8	endif
9	endif
10	endwhile

무작위성을 높이기 위해 기존의 키패드가 가지는 행과 열에 대한 규칙을 제거하였다.

동일 위치점에 대한 방어를 위해 사용자가 입력을 누르는 순간 키보드에 대한 무작위 정렬을 다시 수행하게 된다. 이는 킷값과 입력위치의 관계성을 매 순간순간 재정의함으로써 정보의 유출을 방지하는 기법이다. 하지만 사용자의 키패드가 매 순간 변경되는 것은 사용자의 입장에서 다시 키보드 레이아웃을 학습하여 입력값을 찾아야 하는 문제점을 가진다. 이러한 재학습의 시간을 줄이기 위해 본 논문에서 제시하는 방식은 4개의 열에 대한 초기 진입 index를 사용자에게 알려주어 사용자가 무작위로 입력값을 찾아야 하는 대신 초기 진입 값에서 offset 만큼을 이동하는 indirect 형식의 메모리 접근방식을 사용한다.

따라서 Fig. 1, 2에서와 같이 숫자열 "0~9"는 파란색을 띄며 한번 값에 대한 입력이 수행되면 전체의 열의 배치와 offset이 변경되어 "0~9"의 숫자열은 다른 열에 배치가 되지만 이전의 파란색을 그대로 유지하기 때문에 원하는 문자의 위치를 쉽게 찾아 갈 수 있다. 따라서 제안하는 기법은 무작위로 키를 배치할 때 불가능했던 학습이 가능하도록 설계되어 사용자가 보다 빠르게 원하는 정보를 입력하는 것이 가능하도록 하였다.

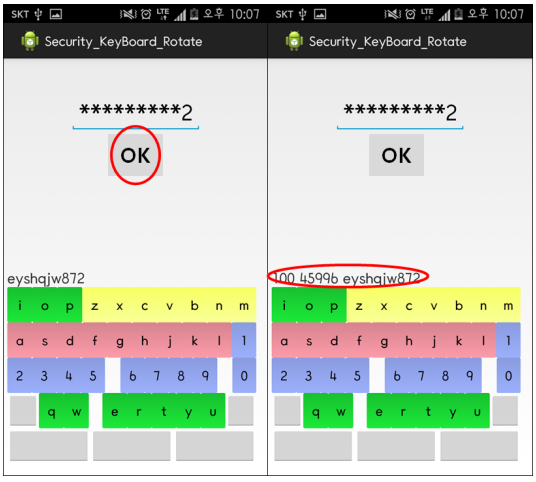

Fig. 2. Test environments of security keyboard (2/2)

IV. 구현 및 성능 평가

본 장에서는 논문에서 제안하는 보안 키패드 기법을 실제 안드로이드 휴대폰에 구현 및 테스트하여 보안성과 신속성 그리고 정확도 측면에서 분석해보도록 한다. 사용된 타겟 보드는 갤럭시 S3 스마트폰으로 선정하였다. 해당 스마트폰은 가장 보편적인 휴대폰으로써 객관적인 도표지출에 적합하다고 생각되어 선택하게 되었다. 본 실험에 참가한 실험자들은 건장한 체격에 시력에 문제가 없으며 기존에 스마트폰을 사용하여 소프트 버튼을 능숙히 사용할 수 있다. 실험에는 총 6명의 실험자가 참가하였다. 테스트한 종목은 총 4개로써 기본형, 무작위형, 무작위 재배열형 그리고 제안된 알고리즘으로 구성된다. 각각의 알고리즘에 대해서는 총 4번의 실험이 이루어지도록 했다.

4.1 신속성

기존 보안키보드의 가장 큰 문제점은 타자입력속도의 저하이다. 기본적인 보안키보드는 일반적인 쿼티 키보드의 레이아웃을 그대로 도입하여 높은 성능을 나타냄을 확인할 수 있다. 하지만 무작위로 배치된 키보드의 경우 사용자 지속적으로 새로운 키보드를 이해해야 하는 문제점을 가진다. 따라서 무작위 키보드의 경우 속도가 느려지게 된다. 하지만 제안하는 기법의 경우 구글글라스 공격을 방어함과 동시에 성능을 효과적으로 향상시켰다. Fig. 3.에서와 같이 무작위로 키보드를 배치하는 키보드 중에서 가장 높은 성능을 나타냄을 확인할 수 있다.

본 논문에서 제시한 기법의 가장 큰 특징은 학습기능이라고 할 수 있다. 제안하는 기법은 사용자가 사전에 알고 있는 쿼티 키보드에 대한 사전지식을 활용할 수 있다. 이와는 달리 무작위로 배치된 키보드를 사용할 때는 사전지식을 확인할 수 없었다. 이는 Fig. 4.에 나타난 보안키보드의 표준편차 값에서 확인해 볼 수 있다. 무작위로 배치하는 기존 보안키보드는 표준편차가 높게 나타남을 확인할 수 있다. 이는 매 입력 순간마다 사용자에게 보안키보드의 난이

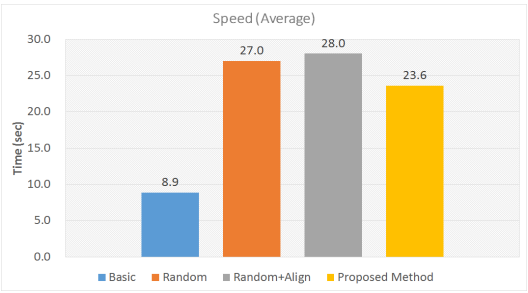

Fig. 3. Comparison of average speed

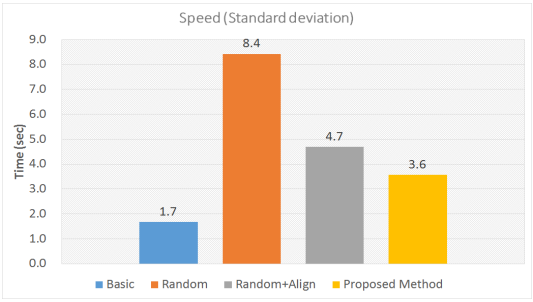

Fig. 4. Comparison of standard deviation

도가 변하게 된다는 것을 의미하며 사용자가 키보드에 친숙해 질 수 없음을 의미한다. 이와는 달리 제안하는 보안키보드는 무작위 보안키보드 중에서 가장 낮은 표준편차를 보임을 확인할 수 있다. 따라서 사용자들이 쉽게 키보드를 인식하고 사용하는 것이 가능함을 나타낸다.

Fig. 5.에서는 기본적인 보안 키보드의 레이아웃에 대한 사전지식의 활용에 대해 확인해 본다. 만약 1, 2를 순서대로 눌러야 하는 상황에서 기본적인 보안 키보드는 1과 2의 위치를 명확하게 알 수 있도록 되어 있다. 따라서 사용자는 원하는 입력을 쉽게 찾아서 적용할 수 있다.

Fig. 6.에는 무작위로 배열된 키보드에 대해 나타내고 있다. 기존의 키보드와는 다른 레이아웃을 가지고 있어서 원하는 1이라는 글자를 처음에 찾는데 많은 시간이 걸린다. 두 번째로 2라는 숫자를 찾을 때도 이전에 1이라는 글자를 찾으면서 발견하지 못했다면 지속적으로 해당 숫자를 찾아야하는 문제를 가진다.

Fig. 7.에는 무작위로 배열된 키보드 레이아웃이 키입력이 발생할 때마다 변경되는 구조이다. 따라서 이전 무작위 배열과 달리 1이라는 숫자를 찾으며 생

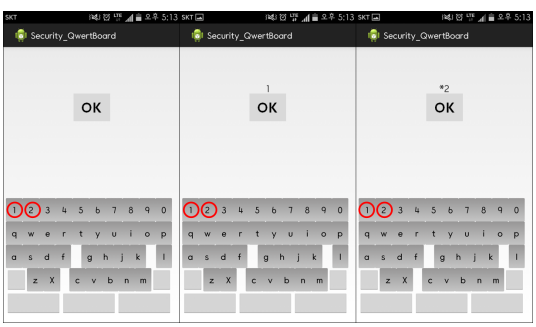

Fig. 5. Basic security keypad

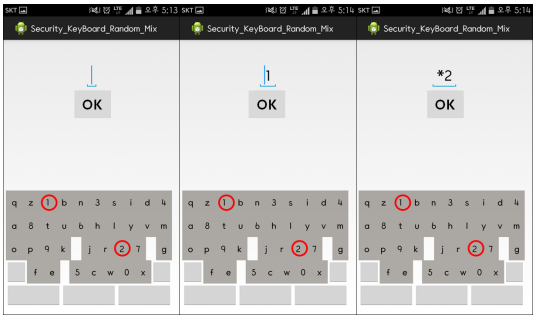

Fig. 6. Random security keypad

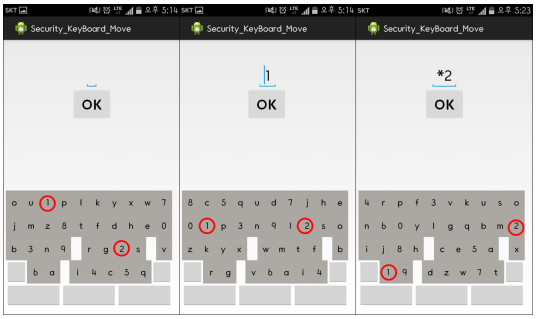

Fig. 7. Random and aligned security keypad

성된 키보드에 대한 지식이 매번 의미가 없어지는 문제점을 가진다. 따라서 그림에서와 같이 첫 번째 입력 때에는 '1'만 두 번째에는 '2'만을 찾아야 의미가 있는 구조이다.

Fig. 8.에는 제안하는 보안키보드가 제시되어 있다. 해당 보안키보드는 파란색이 첫 번째 행인 숫자들의 집합을 나타내게 된다. 따라서 사용자는 4가지의 경우의 수 즉 행의 시작점을 찾으면 '1'이라는 값을 찾을 수 있다. 따라서 무작위의 경우 숫자와 글자의 총합에 대한 복잡도에서 '1'이라는 값을 찾았다면 제안 기법은 행의 개수로 그 복잡도를 줄였다고 할

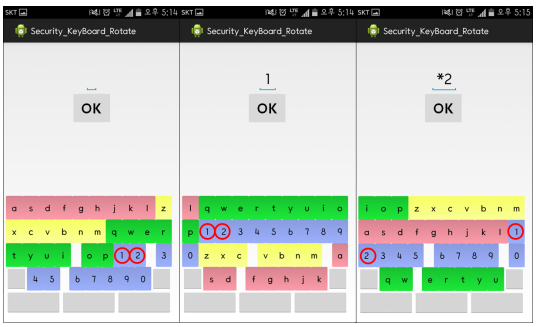

Fig. 8. Proposed security keypad

수 있다. '2'라는 값을 입력할 경우에도 행을 찾은 후 값을 입력하면 되기 때문에 그 효율성이 보다 높다고 할 수 있다. 따라서 해당 기법은 이전의 무작위 기법들과 비교해 사용자가 키보드에 익숙해질수록 신속도가 증가하는 학습능력을 가지고 있다고 할 수 있다.

4.2 정확성

보안성을 향상시킨 보안 키보드는 일반적인 키보드와는 달리 비밀 정보를 숨기거나 생략함으로써 정보 노출을 줄일 수 있는 특징을 가진다. 하지만 제한된 정보를 제공하는 보안키보드는 사용자에게 오타에 대한 피드백 전달이 보안이 적용되지 않은 일반적인 키보드에 비해 잘 진행되지 않는다. Fig. 9.에는 보안 키보드들의 정확도를 나타내고 있다. 본 실험 결과에서는 보안키보드들의 정확도가 100%에 가깝게 나타남을 확인함으로써 실용적인 응용에 문제가 없음을 확인할 수 있었다.

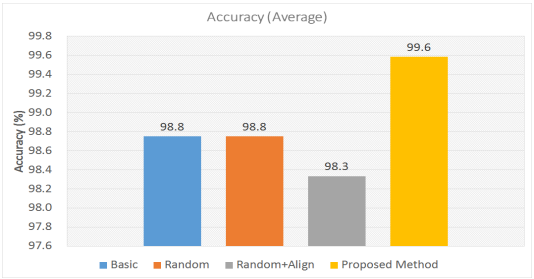

Fig. 9. Comparison of accuracy

4.3 보안성

어깨너머 공격에 대한 보안성은 최근 출시되고 있는 스마트 디바이스인 구글 글라스에 의해 보다 그 중요성이 높아지고 있다. 공격자는 구글 글라스를 사용하여 아무런 제재 없이 사용자의 비밀번호 입력과정을 원거리에서 녹화하는 것이 가능하다. 원거리 상에서의 어깨너머 공격은 사실상 구글 글라스 이전에는 불가능한 공격이었다. 그 이유는 사용자의 눈으로 어림잡아 유추하는 비밀번호의 경우 정확도가 매우 떨어지기 때문이다. 하지만 구글 글라스는 컴퓨팅 파워를 가진 초소형 컴퓨터로써 머신러닝과정을 통해 정확히 비밀번호 유추가 가능한 특성을 가진다. 먼저 기본적인 보안키보드의 경우 구글 글라스를 통한 공격에 노출될 수 있다. 무작위로 키를 배열하는 보안키보드의 경우에는 구글 글라스를 통한 공격에 안전할 수 있다. 하지만 비밀번호 상에 동일한 문자가 포함되는 경우 암호화 복잡도가 줄어들 수 있는 문제점을 가진다. 세 번째로 무작위 문자배열과 재배열의 경우에는 구글 글라스를 통한 공격에 안전하다. 제안하는 기법 또한 문자의 위치와 문자 간에 상관관계가 존재하지 않기 때문에 공격에 안전하다. 보안키보드 간의 보안성 비교는 Table 3.와 같다.

Table 3. Security comparison between methods

	Location prediction	Same character prediction
Basic	○	○
Random	×	○
Random+Align	×	×
Proposed method	×	×

V. 결 론

구글글라스를 통해 수집된 비밀번호 입력 영상에 머신러닝을 적용하면 사용자의 비밀번호 위치점을 쉽게 찾아낼 수 있다. 이를 방지하기 위해 쿼티 키보드의 배치 레이아웃에 대한 정보를 제거하고 무작위로 배치하는 기법이 제시되었다. 하지만 사전 정보의 제거는 키보드 입력이 어렵도록 하는 문제점을 가진다. 이를 효율적으로 해결하기 위해 본 논문에서는 행을 기준으로 인접문자에 대한 사전 정보를 제공하는 기법을 제안한다. 해당 기법은 기존의 보안 키보드와 동일한 보안 강도를 가지지만 입력 신속도는 향상시켜 사용자가 안전하고 편안하게 보안 키보드를 사용하는 것이 가능하게 할 것이다. 또한 학습이 가능한 특징을 통해 사용자가 키보드에 친숙해 질수록 속도가 기본적인 쿼티 키보드와 동일해 질 것으로 예상된다.

References

[1] Yue, Qinggang, Zhen Ling, Xinwen Fu, Benyuan Liu, Wei Yu, and Wei Zhao. "My Google Glass Sees Your Passwords!." Black Hat USA2014, 10(2), pp. 100-103, Aug. 2014.

[2] Gold, Steve. "Electronic counter surveillance strategies," Network Security, 2013(2), pp. 15-18, Feb. 2013.

〈저자소개〉

서 화 정 (Hwa-jeong Seo) 종신회원
2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~현재: 부산대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 암호화 구현, IoT

김 호 원 (Ho-won Kim) 종신회원
1993년 2월: 경북대학교 전자공학과 학사 졸업
1995년 2월: 포항공과대학교 전자전기공학과 석사 졸업
1999년 2월: 포항공과대학교 전자전기공학과 박사 졸업
2008년 2월: 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 3월~현재: 부산대학교 정보컴퓨터공학부 부교수
〈관심분야〉 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안, IoT