



2016 국가암호기술 공모전[II-B. 암호 활용 아이디어 제안]

# 난수를 이용한 Google Glass 상에서의 안전한 PIN 입력방법



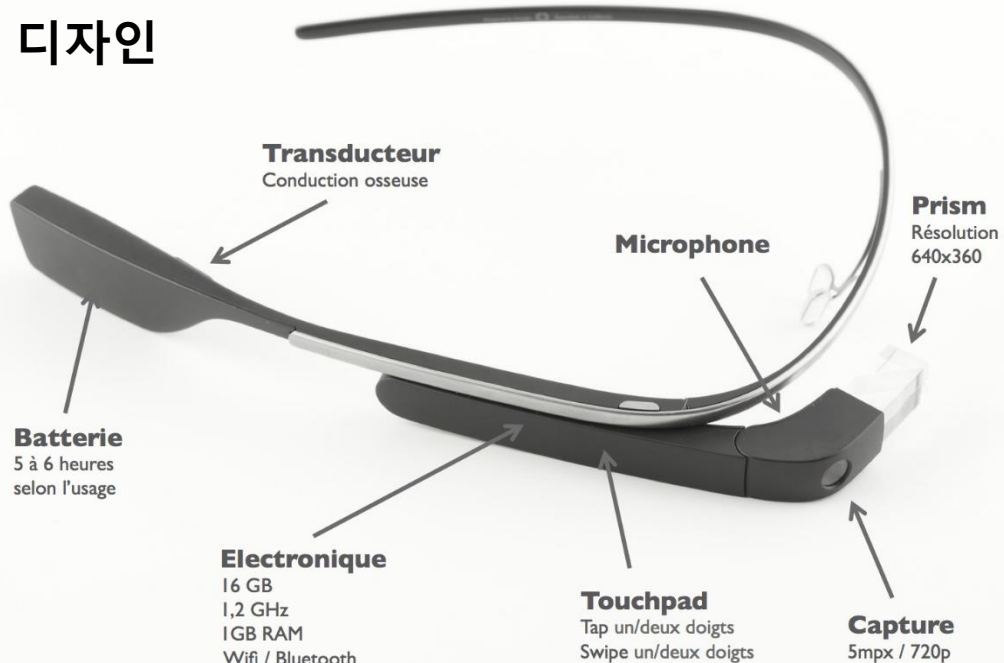


# Google Glass 소개

## 응용 분야



## 디자인



구분	특성
Developer	Google
OS	Glass OS
CPU	OMAP4430
Memory	2GB RAM
Storage	16GB
Display	640 x 360
Controller	Touchpad
Camera	5 Mega
Connectivity	WiFi Bluetooth
Power	570mAh
Weight	36g

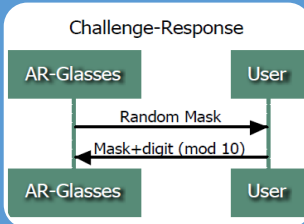
**Google Glass 접근제어:** Google Glass를 통해 다양한 Private 서비스가 가능해 지는 만큼 Google Glass 상에서의 안전한 접근제어 기법 연구가 필요

## Built-in PIN



- 원리: Touchpad로 Touch Pattern 을 입력
- 한계: 긴 입력시간 / 낮은 성공률 / Shoulder-surfing attack

## Bailey et al. [1]



- 원리: 화면의 난수값에 패스워드를 더한 후 10의 나머지 값을 입력
- 한계: 입력값에 대한 feedback이 어려움

## Yadav et al. [2]

1	7	2	5	3	2
4	6	5	0	6	3
7	8	8	1	9	4
		0	9		

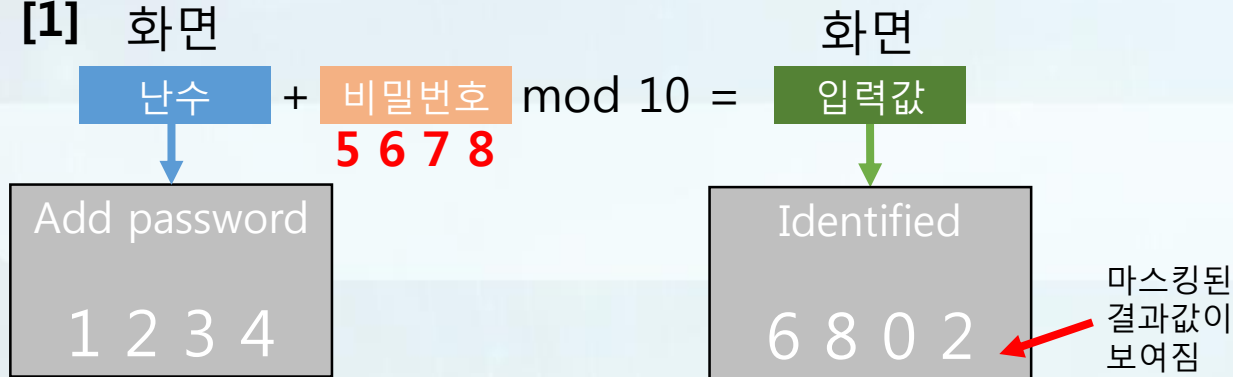
2	8	1
0	3	6
9	4	7
	5	

- 음성 (왼쪽): 두 가지 레이아웃 중 가짜 레이아웃의 입력
- 터치 (오른쪽): 무작위 레이아웃 상에서 값을 입력
- 한계: 긴 입력시간 / 레이아웃을 위한 넓은 스크린 필요



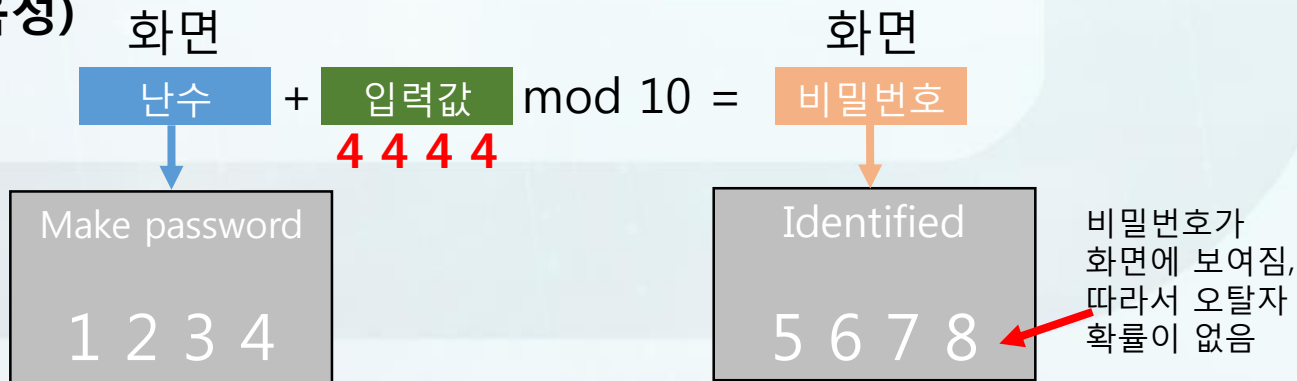
Google Glass 상에서는 음성을 통해 언제 어디서나 사용자가 명령을 내리는 것이 가능, 음성을 이용한 안전한 PIN 입력기술이 활발히 연구되고 있음

## Bailey et al. [1] 화면



----- << 비밀번호가 5678 인 경우 비교 >> -----

## 제안기법 (음성)

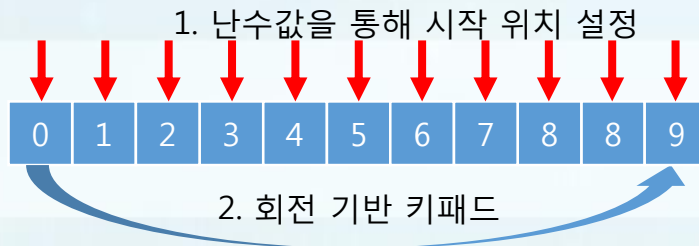


Google Glass는 사용자만이 화면을 볼 수 있으므로 비밀번호가 화면에 노출되더라도 어깨너머 공격에 안전함

## 제안기법 (터치)

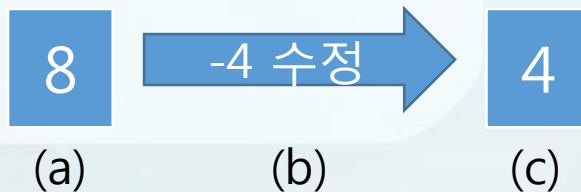
1. 화면 상에 무작위로 선택된 하나의 값을 표기
2. 해당 값을 기준으로 회전 기반 키패드를 통해 입력

- 음성과 달리 입력 값을 사용자가 계산할 필요가 없음
- 입력되는 값에 대한 Feedback을 직관적으로 줌



### << 비밀번호가 4 인 경우 예시 >>

- (a) 초기 난수값이 8로 설정됨
- (b) 값을 -4 만큼 터치 스크롤로 수정
- (c) 비밀번호 4를 입력



해당 과정을 비밀번호의 길이만큼 반복하여 비밀번호를 완성함





**공공 기기 PIN:** ATM과 신용카드 리더와 같이 공공 장소에서 사용되는 PIN Layout은 어깨너머 공격에 취약함, 이를 방지하기 위해 Google Glass에 실제 레이아웃이 오버레이되어 보여지도록 함

1	2	3
4	5	6
7	8	9
*	0	#

기본



1	2	3
4	5	6
7	8	9
*	0	#

결과

## 기존 기법

실사용자와 주위의 모든 사람이 동일한 레이아웃을 공유

1	2	3
4	5	6
7	8	9
*	0	#

기본

+

3	0	6
7	5	2
1	9	4
*	8	#

마스킹



3	0	6
7	5	2
1	9	4
*	8	#

결과

## 제안 기법

사용자만 실제 레이아웃 정보에 Google Glass로 접근

## 동작 예시



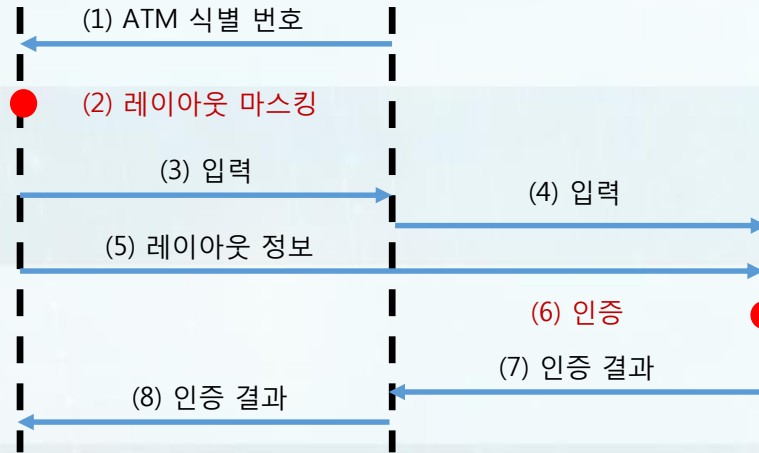
(a) Google Glass 사용자



(b) ATM



(c) 은행 서버



(1) ATM의 식별정보 확인 (ATM의 위치정보, QR코드 혹은 beacon 정보로 확인)

(2, 3) 실제 레이아웃을 Google Glass에 표기하고 입력 시작

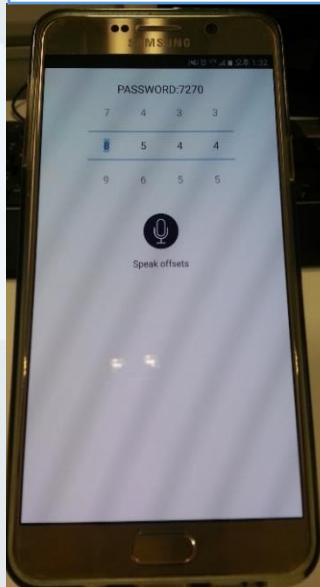
(4, 5) ATM에서는 사용자가 입력한 위치 정보만을 은행서버로 전송하고 사용자는 레이아웃만 전송

(6) 두 정보를 종합하여 비밀번호를 도출 및 인증

(7, 8) 인증결과를 ATM과 사용자에게 전달



구분	특성
Developer	Samsung
OS	Android OS
CPU	Exynos 7420
Display	1440 x 2560



Google Glass PIN



공공기기 PIN

## 프로토타입 구현 환경

- 안드로이드 스마트 폰 (Galaxy Note5) 사용
- Google Glass의 특징인 Shoulder-surfing에 안전한 스크린을 고려하여 스마트폰의 스크린은 사용자만 볼 수 있다고 가정

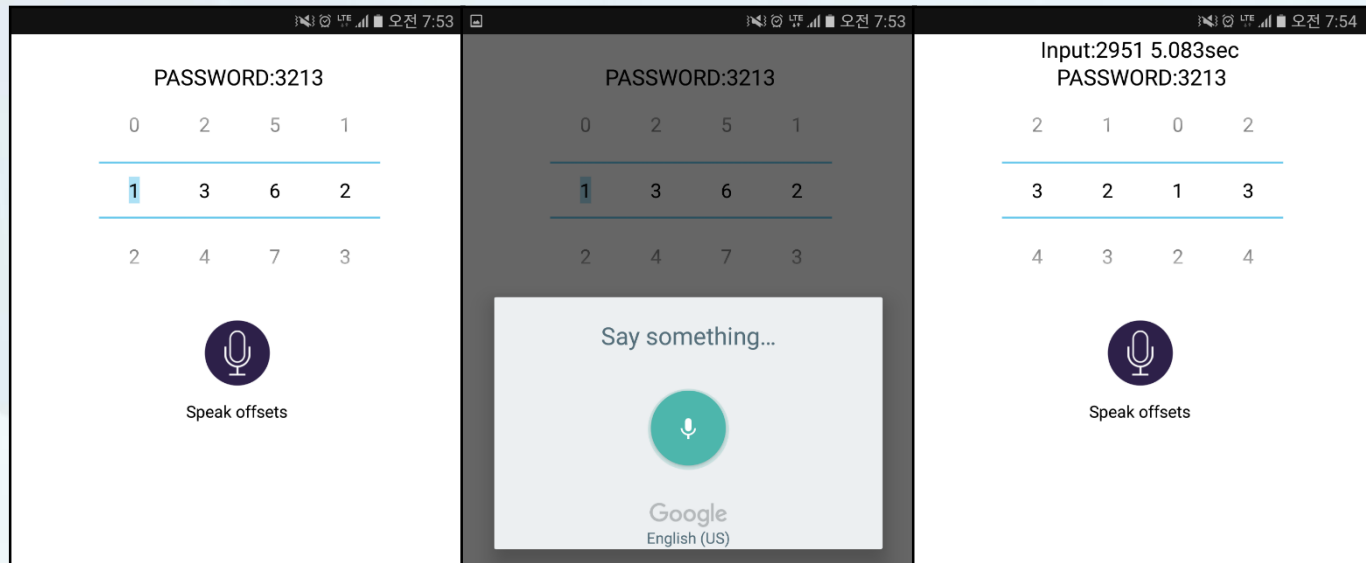
## 구현 상세

- 난수 생성: Java 라이브러리 (java.util.Random)
- 음성 인식: android 라이브러리 (android.speech.RecognizerIntent)
- 오버레이 이미지 구현: 오픈소스 (<https://github.com/SeptiyanAndika/Camera-Overlay-Android>)

## 구현 방법

- 총 10명의 사용자에게 10번의 수행을 시도 후 평균값 도출
- 총 4자리의 비밀번호를 입력하도록 함

# 데모 구현: Google Glass PIN (음성)



(a)

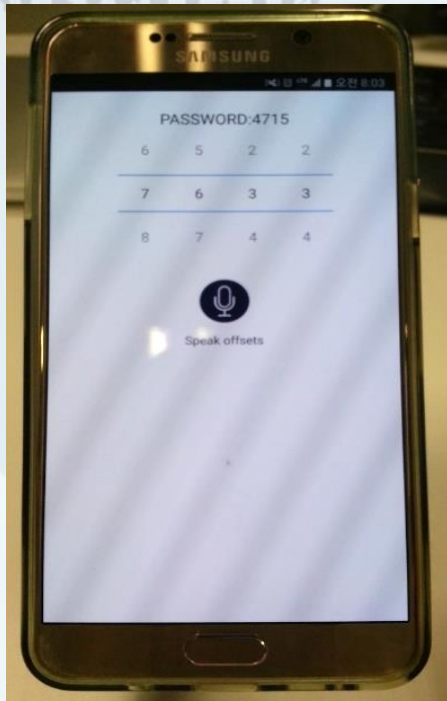
(b)

(c)

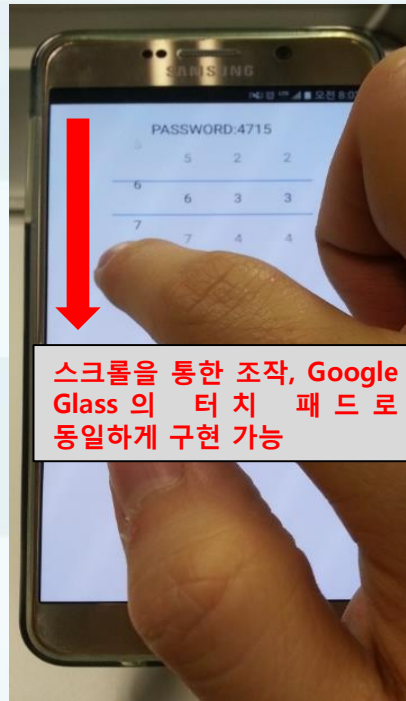
- (a) 비밀번호 3213을 입력하기 위한 초기 상태화면으로써 난수값은 1362로 설정된 상태  
(b) 난수값 1362로부터 비밀번호 3213 값을 도출해 내기 위해 수정값 2951 을 음성으로 전달  
(c) 전달된 수정값 2951을 통해 난수값 1362로부터 3213이 도출

$$\begin{aligned}(1 + 2) \bmod 10 &= 3 \\(3 + 9) \bmod 10 &= 2 \\(6 + 5) \bmod 10 &= 1 \\(2 + 1) \bmod 10 &= 3\end{aligned}$$

# 데모 구현: Google Glass PIN (터치)



(a)



(b)



(c)

- (a) 비밀번호 4715을 입력하기 위한 초기 상태화면으로써 난수값은 7633으로 설정된 상태
- (b) 첫번째 숫자 7에서 터치 스크린을 스크롤하여 입력 숫자를 조정
- (c) 첫번째 숫자를 4로 맞춤, 나머지 숫자도 동일한 방식으로 수정가능

# 데모 구현: 공공기기 PIN



(a)



(b)



(c)

구분	(a)	(b)	(c)
공공기기 (흰색숫자): 0123456789	9	1	5
실제 (주황색숫자): 4983721065	5	9	2

# 제안기법의 사용 용이성 평가

기법	입력	사용 용이성			보안		
		시간 (sec)	성공률 (%)	다중 입력	P <sub>GA</sub>	P <sub>RA</sub>	P <sub>CA</sub>
Google Glass PIN							
Built-in	터치	5.6	68	X	0.0001	1	0.0001
VBP [2]	음성	6.4	83	X	0.0001	0.0001	0.0001
TBP [2]	터치	13.9	87	X	0.0001	0.0001	0.0001
제안 v1	음성	4.8	100	O	0.0001	0.0001	0.0001
제안 v2	터치	5.8	100	X	0.0001	0.0001	0.0001
공공 기기 PIN							
기본	터치	2.2	90	X	0.0001	1	0.0001
제안	터치	5.3	85	X	0.0001	0.0001	0.0001

**Google Glass PIN:** 사용자의 비밀번호가 상시 스크린에 노출 (높은 성공률), 다중 입력가능 (음성), [1] 기법은 논문에서 실험결과가 제공되지 않음, 다만 입력 방식이 유사하여 입력 시간은 큰 차이가 없겠지만 입력 성공률에서는 제안한 기법 (feedback)이 월등히 높을 수 밖에 없음

**공공 기기 PIN:** 마스크 적용으로 인해 기본적인 기법에 비해 입력시간과 성공률이 떨어짐



기법	입력	사용 용이성			보안		
		시간 (sec)	성공률 (%)	다중 입력	$P_{GA}$	$P_{RA}$	$P_{CA}$
Google Glass PIN							
Built-in	터치	5.6	68	X	0.0001	1	0.0001
VBP [2]	음성	6.4	83	X	0.0001	0.0001	0.0001
TBP [2]	터치	13.9	87	X	0.0001	0.0001	0.0001
제안 v1	음성	4.8	100	O	0.0001	0.0001	0.0001
제안 v2	터치	5.8	100	X	0.0001	0.0001	0.0001
공공 기기 PIN							
기본	터치	2.2	90	X	0.0001	1	0.0001
제안	터치	5.3	85	X	0.0001	0.0001	0.0001

\* $P_{GA}$ : 비밀번호 추측 확률  $P_{RA}$ : 비밀번호 입력 화면 녹화 후 추측 확률  $P_{CA}$ : 비밀번호 입력을 수 차례 실시 후 추측 확률

**Google Glass PIN:** 비밀번호가 고르게 분포됨, 사용자의 입력 장면에서 비밀번호 노출 방지, 입력에 대한 Response에서 비밀번호 정보 미포함, 따라서 3개의 보안 관점에서 안전성을 확보


**공공 기기 PIN:** 마찬가지로 사용자의 비밀번호가 노출되지 않아 안전함



Q & A



감사합니다

- 
- [1] D. V. Bailey, M. Durmuth, and C. Paar. “typing passwords with voice recognition: How to authenticate to Google Glass,” In *Proc. of the Symposium on Usable Privacy and Security*, 2014.
- [2] D. K. Yadav, B. Ionascu, S. V. K. Ongole, A. Roy, and N. Memon. “Design and analysis of shoulder surfing resistant PIN based authentication mechanisms on Google Glass,” In *Financial Cryptography and Data Security*, pages 281-297. Springer, 2015.

## Google Glass PIN (음성 기반)

Input : 난수값  $R$ , 수정값  $C$

Output: 결과값  $V$

1. 난수값  $R$  생성
2. 사용자가 음성을 통해 수정값  $C$  입력
3. 결과값 ( $V = R + C$ ) 도출 (값 수정 알고리즘 참고)
4. 만약 결과값이 비밀번호이면 결과값  $V$  출력
5. 다르면 결과값을 난수값으로 설정 후 Step 2부터 다시 수행

## 값 수정 알고리즘 (4자리 입력의 경우)

Input : 난수값  $R$  ( $R[3], R[2], R[1], R[0]$ ), 수정값  $C$  ( $C[3], C[2], C[1], C[0]$ )

Output: 결과값  $V$  ( $V[3], V[2], V[1], V[0]$ )

1.  $V[0] = (R[0] + C[0]) \bmod 10$  (일의 자리)
2.  $V[1] = (R[1] + C[1]) \bmod 10$  (십의 자리)
3.  $V[2] = (R[2] + C[2]) \bmod 10$  (백의 자리)
4.  $V[3] = (R[3] + C[3]) \bmod 10$  (천의 자리)