연세대학교 정보보호연구실
INFORMATION SECURITY LAB @ GSI
YONSEI UNIVERSITY, SEOUL, KOREA

모바일 인증을 위한 직관적 편리한 HCI 기반 인증기술

2015. 08. 27

연세대학교 권태경

Email: taekyoung@yonsei.ac.kr

스마트폰 사용자 인터페이스 위협 모델

Xu et al., WiSec, 2009

Matsumoto and IMAI, EUROCRYPT, 1991

Aviv et al., USENIX WOOT, 2010

안전한 인증 인터페이스 개발

스머지 저항 기법	숄더 서핑, 레코딩 저항 기법	스파이 저항 기법
TinyLock	SteganoPIN/SwitchPIN	RIK

스머지 공격

- 안드로이드 패턴락을 통해 입력된 비밀 패턴이 터치스크린에 그대로 남아 있는 문제가 있음. 이를 통해 입력 패턴을 유추하는 공격이 가능함

패턴 'G' 입력

지문 방지 필름을 사용해도 패턴 입력 흔적이 남음

패턴 입력 흔적

*AJ. Aviv, K. Gibson, E. Mossop, M. Blaze, and JM. Smith, "Smudge Attacks on Smartphone Touch Screens," in Proc. 4th USENIX Conference on Offensive Technologies (WOOT), 2010

숄더 서핑 공격

- **Human Shoulder-surfing**:
  모바일 기기 특성상, 공공 장소에서 자주 사용하게 되며, 특히 사용자 인증을 위해 비밀값을 입력하는 경우 주변에서 쉽게 엿볼 수 있음

- **Camera-based Shoulder-surfing**:
  디지털 카메라, 스마트기기 등 부가적인 레코딩 장치를 이용하여 사용자의 비밀값 입력을 녹화하는 공격이 가능함

*T. Matsumoto and H. IMAI, "Human Identification Through Insecure Channel," in Proc. EUROCRYPT, 1991

스마트폰 스파이웨어

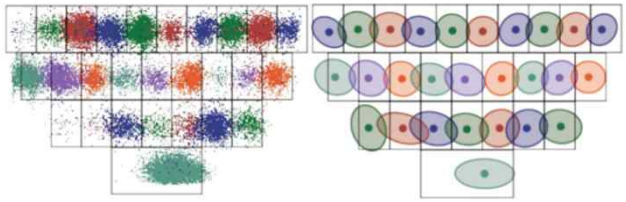
- 사용자 몰래 스마트폰에서 개인 정보 및 모바일 사용 정보를 수집함
- 민감한 개인 정보 및 행동 정보(터치 이벤트, 스크린 캡쳐)를 수집할 수 있음

<iKeyMonitor>

1초마다 스크린 화면을 가져올 수 있음

<가상 키보드 스크린 캡쳐>

<랜덤 공백 키보드 스크린 캡쳐>



*출처: The Hacker News

*N. Xu, F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng, "Stealthy Video Capturer: A New Video-based Spyware in 3G Smartphones," in Proc. ACM Conference on Wireless Network Security (WiSec), 2009

터치스크린 탑재 기기 증가

Usable Security

Useful — Secure knowledge-based authentication

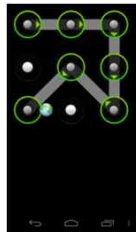
Usable — Fast and easy procedures, Simple operations, and Small memory

Used — Standard input methods

Usability  **Security**

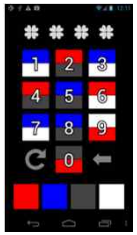
핵심 기술

스머지 저항 인증 시스템

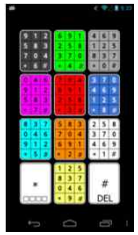

<S-Lock>


<TinyLock>

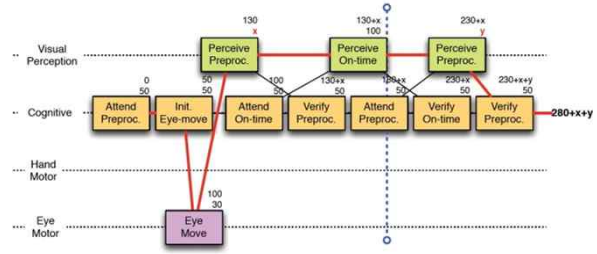
숄더 서핑 저항 인증 시스템


<4 Color>


<PassPath>


<Quick PassPath>

정형 모델링

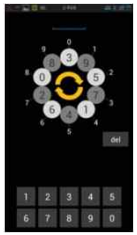


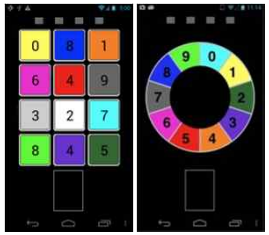
<STM-GOMS>

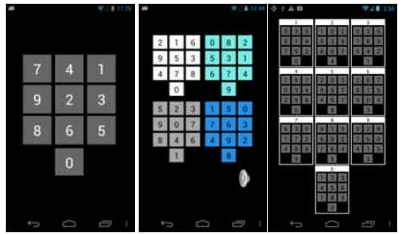
스킨형 사용자 인터페이스

<TPointer>


<Drag & Type>


<CountPIN>


<S-PIN+ Pad>


<SwitchPIN>

<HiddenEnter>

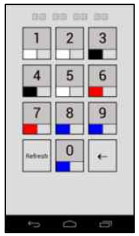

<LIN3D>

스파이 저항 인증 시스템


<Secure DnT>


<RIK>

레코딩 저항 인증 시스템


<TictocPIN>


<CupPIN>


<ColorDotPIN>


<SwitchPIN>

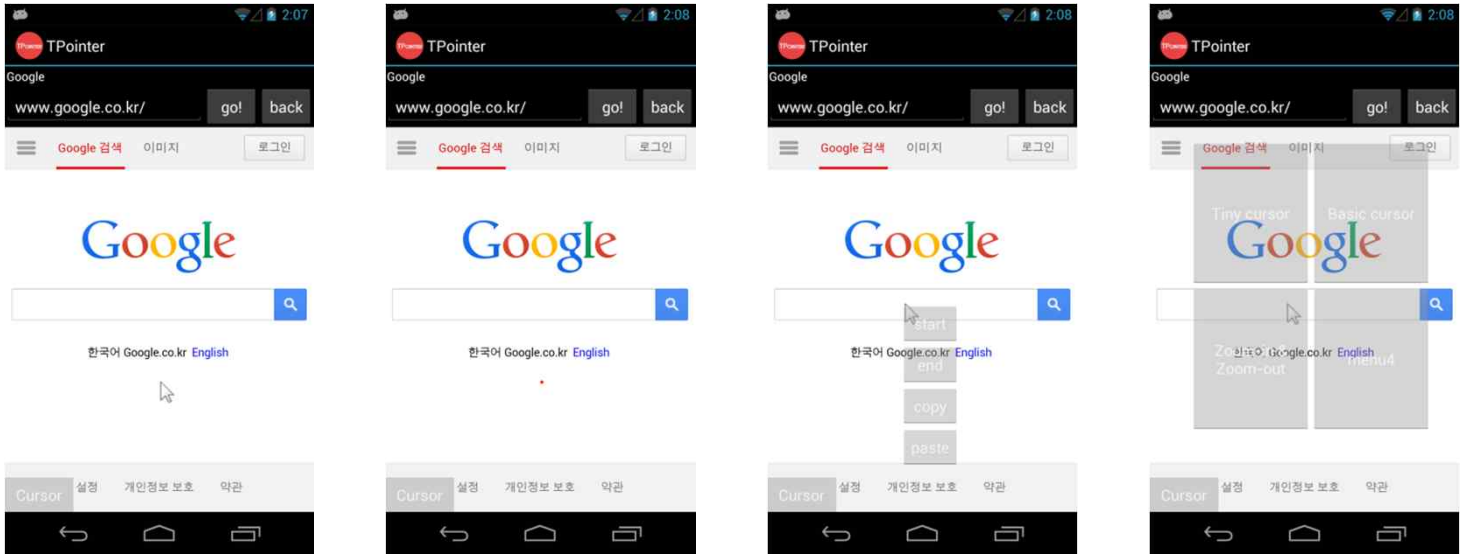

<PassSlot>


<SteganoPIN>

사용자 인터페이스

❖ TPointer (Kwon et al., IEEE TCE, 2014)*

- 작은 터치스크린에서 정확한 터치 조작을 위해 개발된 가상 포인터 기반의 인터페이스
- offset-free 포인터 기반의 point-and-click 방식을 사용하여 정밀하면서도 다양한 터치 기능 제공

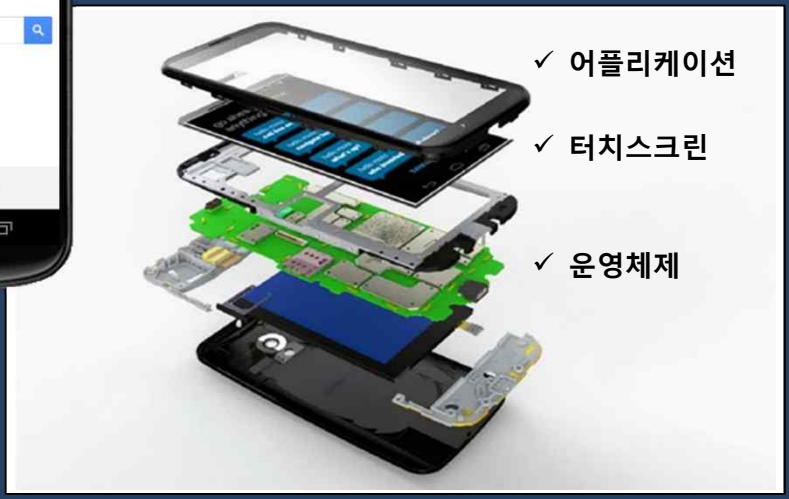


포인터 활성화 | 미세 포인팅 | 우클릭 메뉴 | 확장 메뉴

*T. Kwon, S. Na, and Sooyeon Shin, "Touch Pointer: Rethink Point-and-Click for Accurate Indirect Touch Interactions on Small Touchscreens," IEEE Trans. on Consumer Electronics, 2014

개발 기술 활용 방안

- 고해상도 스마트폰이나 터치스크린 기반의 스마트기기에서 빠르고 정확한 터치 입력을 위해 활용
- 스마트폰 등 스마트기기의 부가 기능으로 사업화

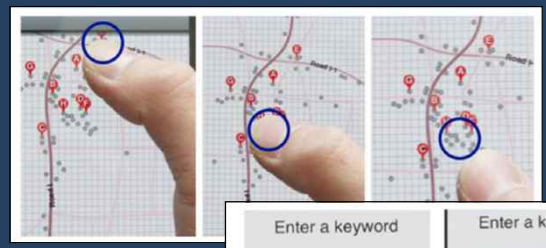


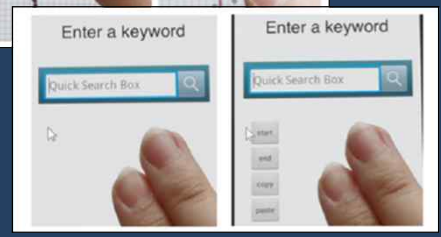
✓ 어플리케이션

✓ 터치스크린

✓ 운영체제

지도 앱



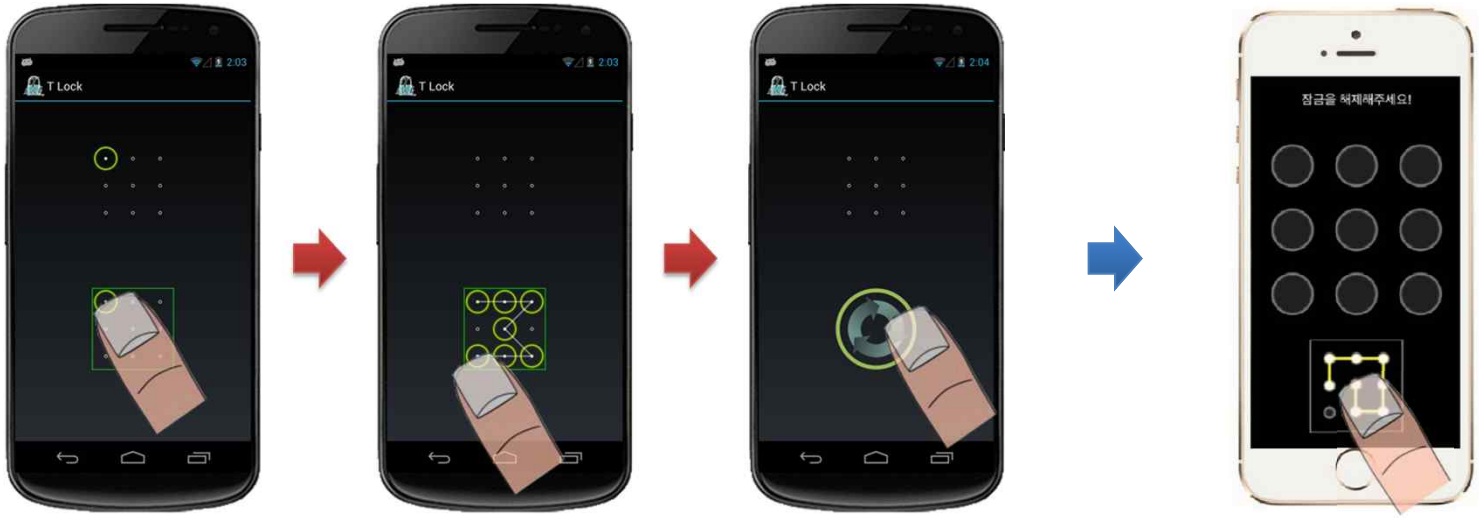


웹 브라우저

스머지 저항 인증 기술

❖ TinyLock (Kwon and Na, Computer & Security, 2014)*

- 스머지 공격과 숄더 서핑 공격에 저항 가능한 패턴 입력 기법



아이폰 버전

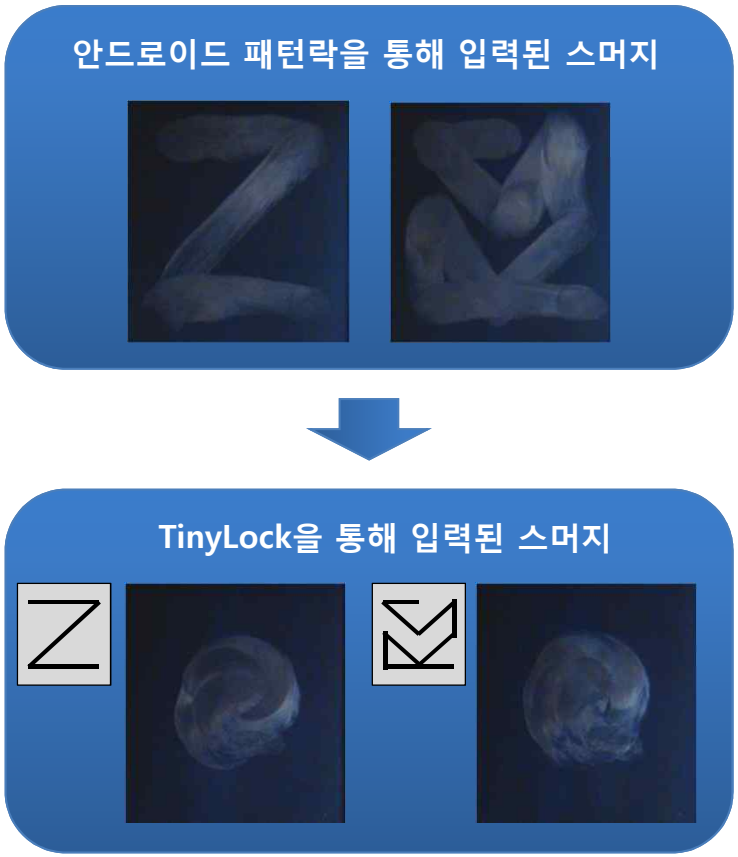
- 스머지 공격 **100% 저항**
- 모바일 인증의 공격 저항을 위한 소요시간: **2-4초**
- 정상 사용자의 입력 오류율: **2%**

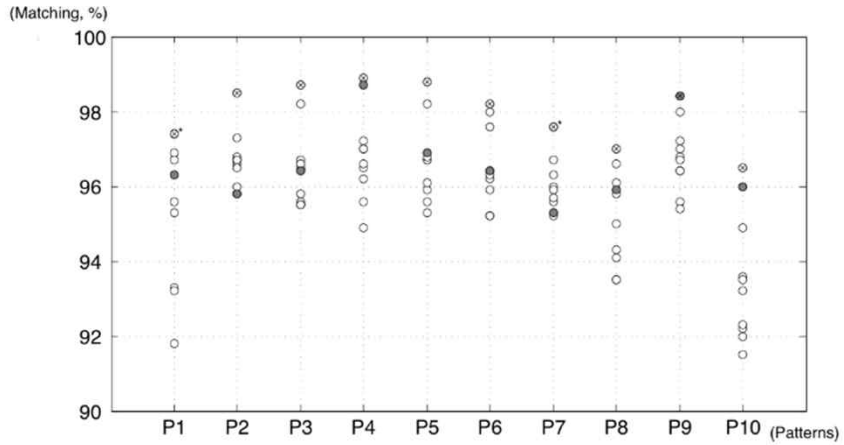
*T. Kwon and S. Na, "TinyLock: Affordable Defense Against Smudge Attacks on Smartphone Pattern Lock Systems," Computers & Security, 2014

스머지 저항 인증 기술

❖ TinyLock – 안전성 분석

- 스머지(입력 패턴) 비교 분석 결과

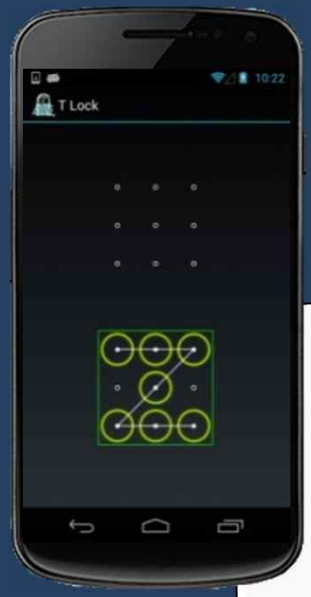




- **동일 패턴에 대한 스머지인지 판별 어려움**
- **다른 패턴에 대한 스머지가 같을 수 있음**

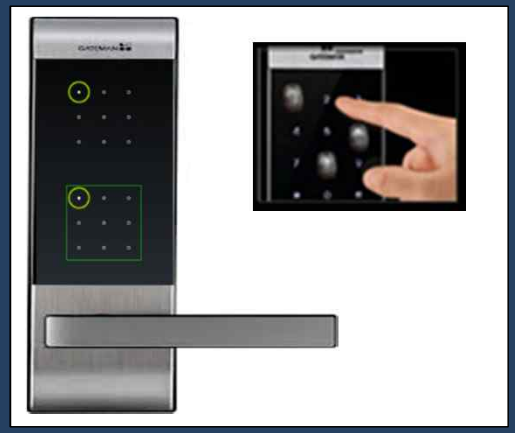
??

개발 기술 활용 방안



- 스머지, 숄더 서핑 공격에 강인한 터치스크린 기반의 그래픽 패스워드 인증 수단으로 활용
- 스마트폰 부가 기능, 도어락 인증 수단으로 사업화

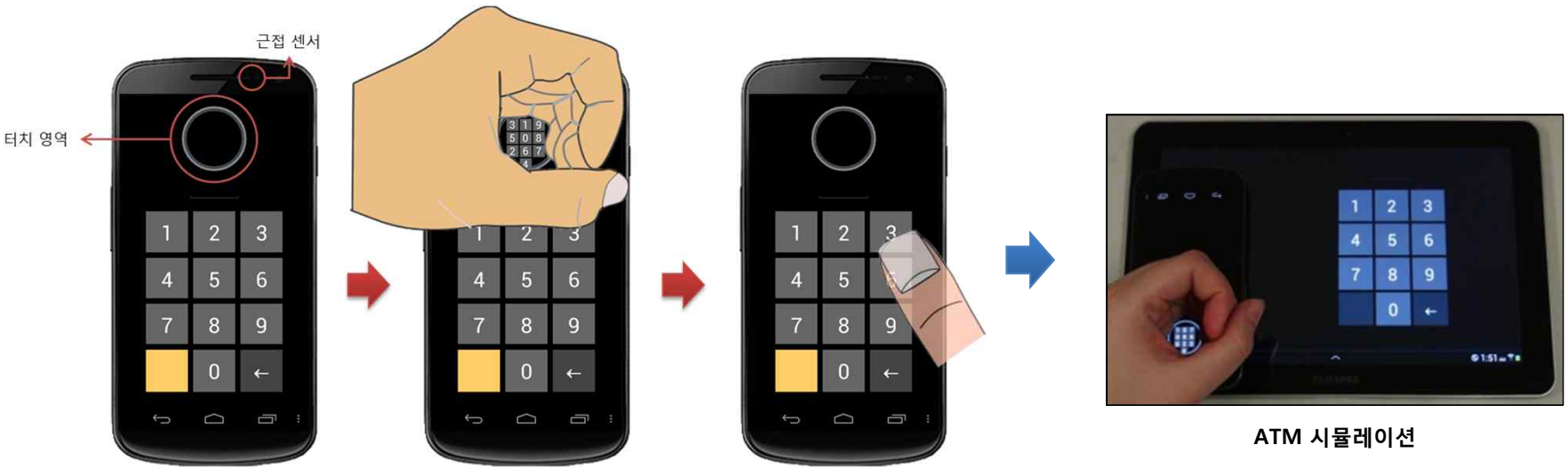
디지털 도어락 적용



숄더 서핑 저항 인증 기술

❖ SteganoPIN (Kwon and Na, IEEE THMS, Accepted)*

- 카메라 기반의 숄더 서핑 공격에 저항 가능한 비밀번호 입력 기법



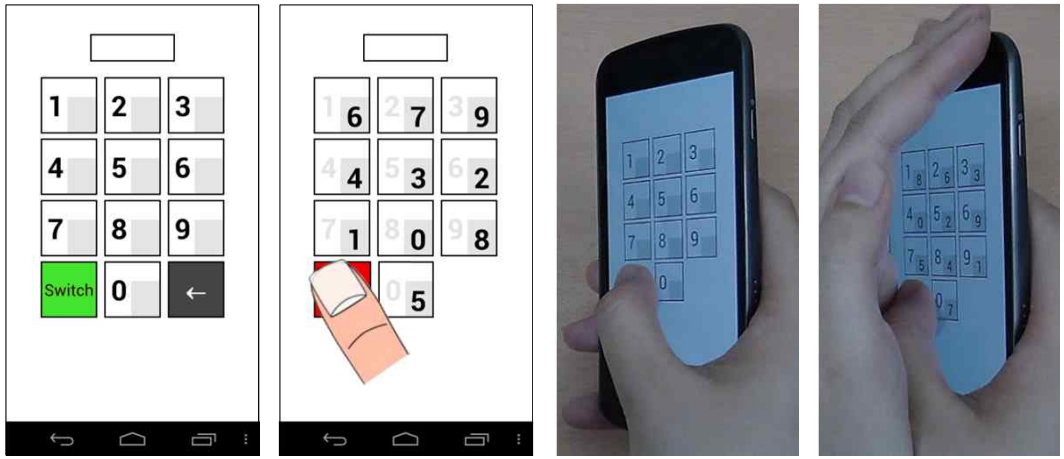
- 카메라 기반의 숄더 서핑 공격에 **99% 저항**
- 모바일 인증의 공격 저항을 위한 소요시간: **3-4초(5-6초)**
- 정상 사용자의 입력 오류율: **2%**

*T. Kwon and S. Na, "SteganoPIN: Two-Faced Human-Machine Interface for Practical Enforcement of PIN Entry Security" IEEE Trans. on Human-Machine Systems, 2015 (Accepted)

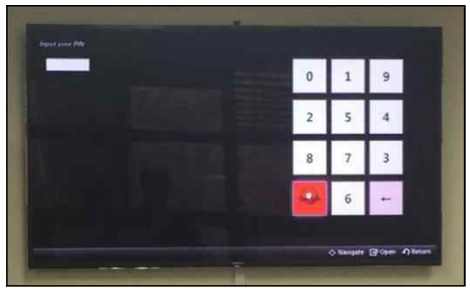
숄더 서핑 저항 인증 기술

❖ SwitchPIN (Kwon and Na, IEEE ICCE, 2014)*

- 카메라 기반의 숄더 서핑 공격에 저항 가능한 비밀번호 입력 기법



레코딩 공격에 저항하기 위한
물리적 보호 기술 추가

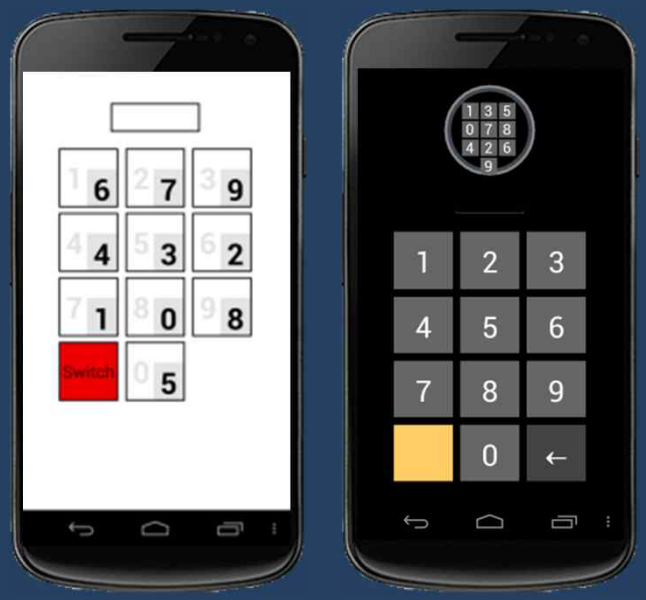


스마트TV 버전

- 카메라 기반의 숄더 서핑 공격에 **99% 저항**
- 모바일 인증의 공격 저항을 위한 소요시간: **4-5초**
- 정상 사용자의 입력 오류율: **2%**

*T. Kwon and S. Na, "SwitchPIN: Securing Smartphone PIN Entry with Switchable Keypads," in Proc. IEEE International Conference on Consumer Electronics (ICCE), 2014 (저널 버전 준비 중)

개발 기술 활용 방안



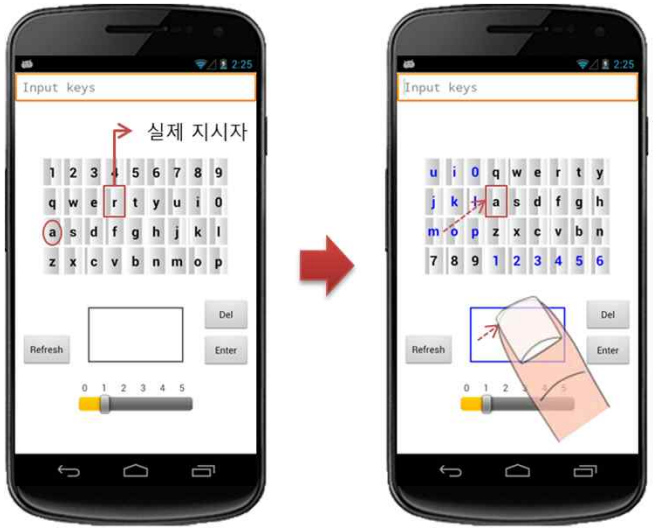
단말 시스템 적용

- 숄더 서핑 공격, 레코딩 공격에 강인한 터치스크린 기반 PIN 입력 수단으로 활용
- ATM 기기, PoS 터미널을 위한 PIN 입력 관련 기술 사업화

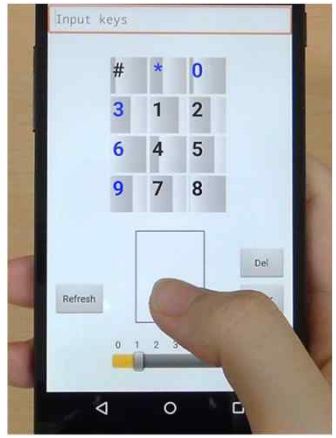
스파이 저항 인증 기술

❖ RIK (Na and Kwon, IEEE ICCE, 2014)*

- 연속 스크린 캡쳐 공격을 수행하는 스파이웨어에 저항 가능한 패스워드 입력 기법



Password-based RIK



PIN-based RIK

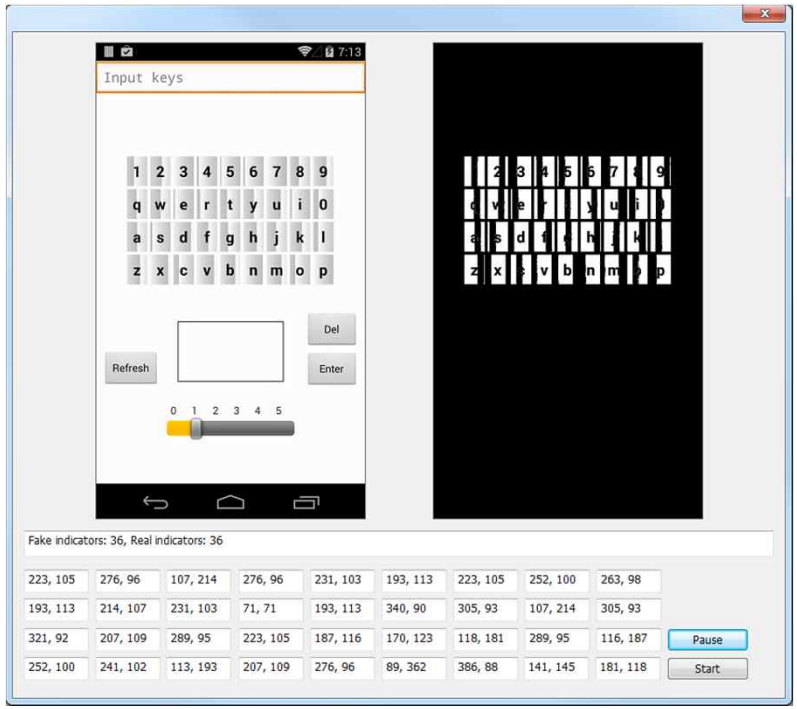
- 스파이웨어 공격(14 shots/s 스크린 캡쳐 공격 수행)에 **99% 저항**
- 모바일 인증의 공격 저항을 위한 소요시간: **8-9초(26-27초)**
- 정상 사용자의 입력 오류율: **0%(3%)**

*S. Na and T. Kwon, "RIK: A Virtual Keyboard Resilient to Spyware in Smartphones," in Proc. IEEE International Conference on Consumer Electronics (ICCE), 2014 (저널 버전 심사 중)

스파이 저항 인증 기술

❖ RIK – 안전성 분석

- 연속 스크린 캡쳐 공격을 수행하여 입력 문자를 알아내고자 함
- 동적 이미지의 이동 패턴 일부는 알 수 있었지만, 이를 통해 실제 지시자의 위치는 찾을 수 없음
- 실제 지시자의 위치를 알 수 없기 때문에 입력 문자를 알아내는데 실패함
- 스크린 캡쳐 공격을 수행하는 스파이웨어에 저항 가능함



- 실제 지시자 위치: `h'

개발 기술 활용 방안

금융 앱에 활용

보안 키보드

- 스파이웨어 공격에 강인한 터치스크린 기반 PIN/패스워드 입력 수단으로 활용
- 핀테크(Fintech) 및 뱅킹 앱을 위한 인증 기술 사업화

Q&A