Information Security Engineering

2017.09.20

可用安全

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

Usable Security

Overview

可用性

- It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals match the mechanisms he must use, mistakes will be minimized.

—Proc. IEEE 1975

- The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.

—ISO 9241-11: 1989

Usable Security

可用安全

- Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future."

—Computing Research Association 2003

- 对于安全问题，技术不能提供全部的解决方案，人的因素一直被忽视，安全研究人员并不非常关心用户需要什么

- 我们需要考量用户如何同系统进行交互
- 结合HCI（人机接口）与信息安全
- 超越UI：改变用户和开发者习惯和思路

为什么需要可用安全

- 安全系统是复杂的，必定是不完美的，软件一定有bug，安全的更多

- 安全增加了障碍： If you want security, you must be prepared foe inconvenience

- 安全是风险管理，必须平衡损失和花费，但损失和花费难于测量

- 用户不理解数据、软件和系统的重要性
- 用户不了解什么资产处在危险中
- 用户不理解他们的行为处在风险中

- 教育训练
- 设计一个可用的安全系统

可用安全面临挑战

- 安全是次要任务，没有人买计算机是为了安全
- 配置安全工具的时间对于用户来说是“白白浪费”

- 安全系统和方案经常是比较复杂的，用户难于理解，执行经常出现错误

- 用户不知道是什么时间和如何执行安全相关的任务
- 用户没有动机执行安全相关的任务
- 用户没有能力做安全决策

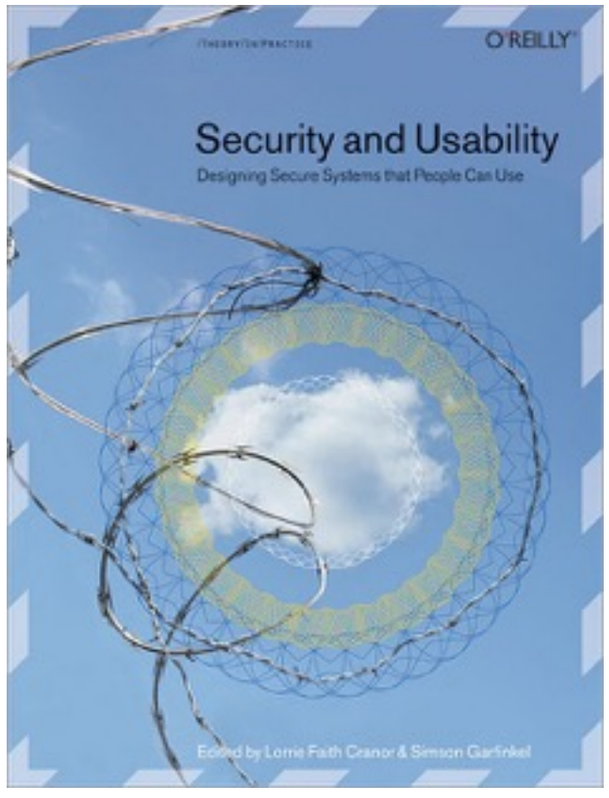
起源

- **User-Centered Security**, *NSPW 1996*
- **User Are Not the Enemy**, *CACM 1999*
- **Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0**, *USENIX Security, 1999*

July 6-8, 2005
Pittsburgh, PA

Symposium on Usable Privacy and Security

Security and Usability: Designing Secure Systems that People Can Use



可用安全的目标

- 对于需要执行的安全任务是可靠的
- 能指出如何成功的执行安全任务
- 不会出现危险的错误
- 使用和交互中足够舒适

用户为中心的设计

- 安全不可见
- 安全和意思可理解
- 训练用户
- 不期望用户做一些用户无法选择的决定
- 自动化系统更加可预期和准确

用户和安全拥有足够的通信

安全不可见

- 让安全机制不可见
- 成功案例：SSH、SSL、VPN、自动更新、IBE

- 但是方便容易带来威胁

安全与隐私可理解

- 安全与隐私可见
- 安全与隐私更直观
- 帮助用户做安全决策

- 用户是否理解，是否注意
- 用户是否了解安全机制
- 用户是否实际去做，是否会持续去做

一个例子： Privacy Bird

- Web站点隐私策略

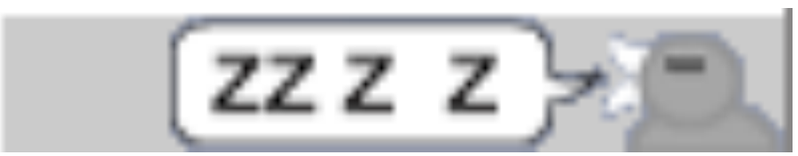
✳很多，但用户很少读

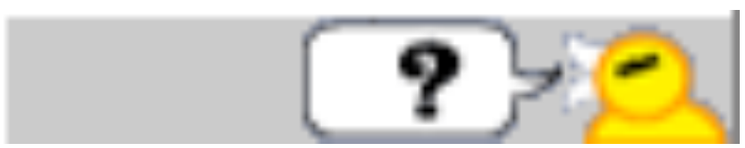
- Privacy Bird

✳决定是否站点策略和用户隐私策略项匹配

✳通知用户

http://www.privacybird.org/



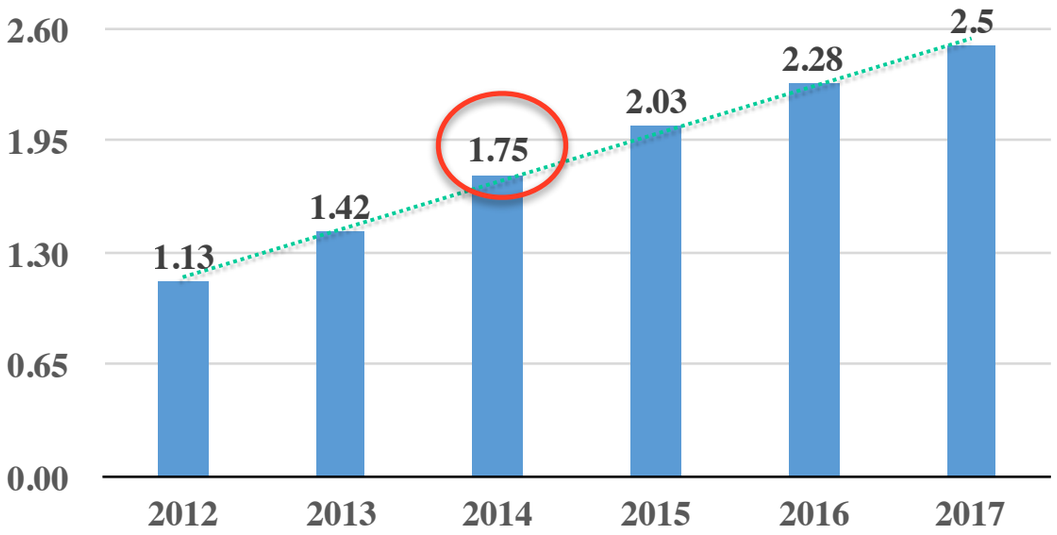


SlidePIN:

Slide-based PIN Entry Mechanism on Smartphones

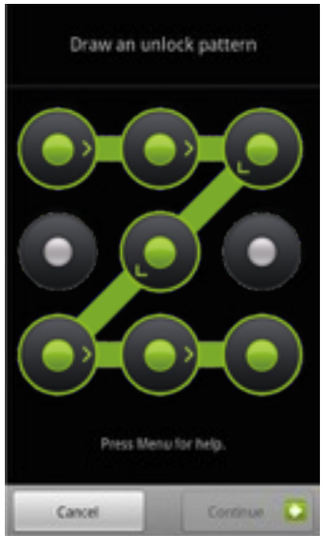
背景

www.eMarketer.com



4 digits PIN

PatternLock



No

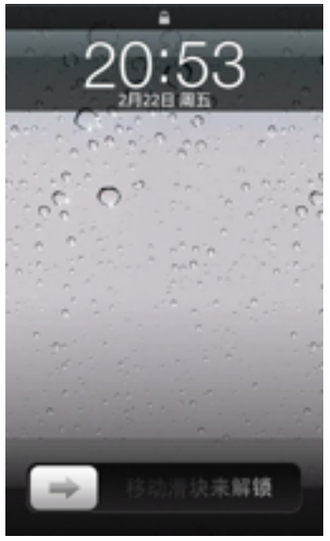
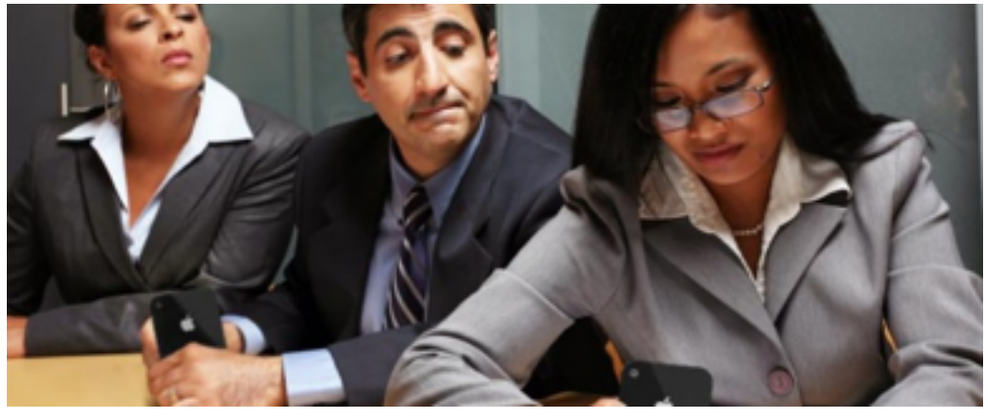


Photo Audio Video
SMS Call Email
Payment Location
SNS Blog IM
… …

http://www.mireview.com/blog/wp-content/uploads/2013/03/timthumb.jpg

Shoulder surfing attack



什么是肩窥攻击

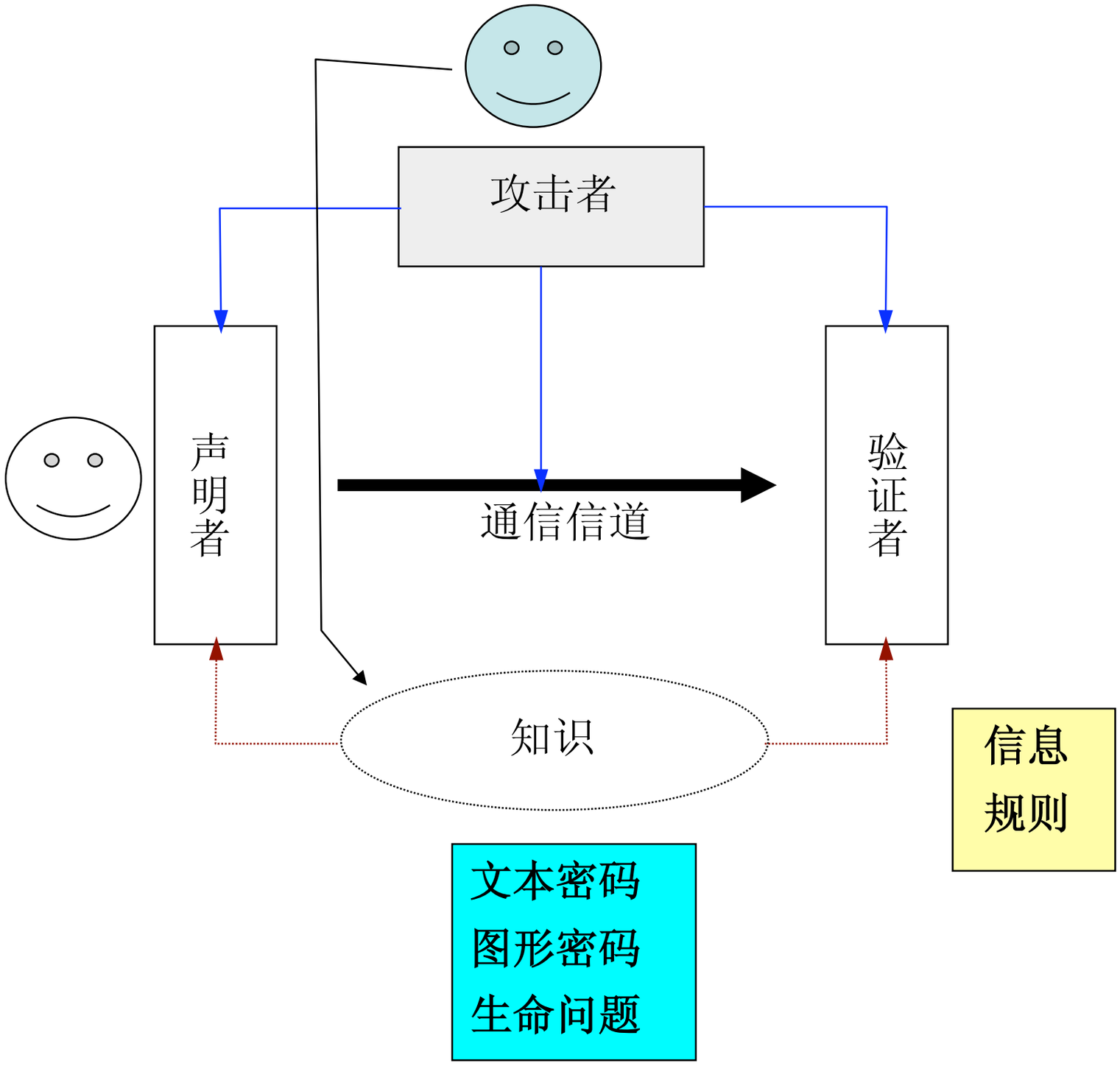
- 肩窥攻击（Shoulder Surfing）也称为窥视攻击，是一种利用直接观察就可以得到所需要信息的攻击技术，是社会工程的一种，对于基于知识的身份认证机制有着非常大的威胁，特别对于文本密码、图形密码和隐私问题这三个最主要的认证机制。

- 肩窥攻击一般发生在相对临近的环境中，特别是在比较拥挤的地方，在这种环境中攻击者可以很容易的看见临近的一些人所填写的标单、在ATM机器上录入的PIN、在公用电话上使用的电话卡、在屏幕上显示得各种信息等。当然在摄像头、望远镜、录像机等设备的支持下，肩窥也能发生在非常远的距离。

- 肩窥攻击基本上有四种形式：临近偷看、使用设备、声学跟踪、电磁泄露。

- 该类攻击被人提及已有20多年的历史，但一直没有引起足够的重视，现有的相关研究和论文还不太多。但是随着移动网络和移动计算的发展，越来越得到了重视。

肩窥攻击产生原因



相关工作

Computing burden

Memory burden

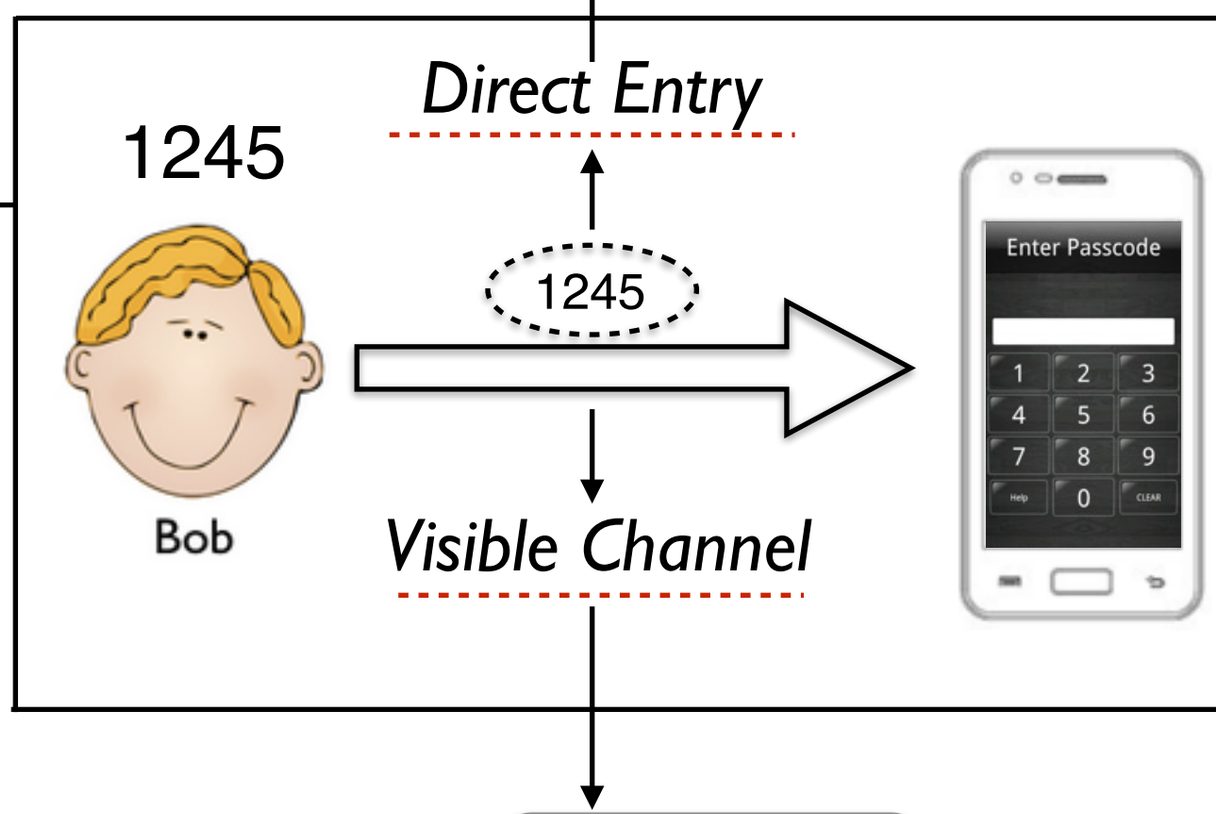
Indirect Entry Mechanism

Human-computable challenge-response

Challenge

- *Keypad layout*
- *Additional factors*
  - ☆ *Colors*
  - ☆ *Symbols*
  - ☆ *Directions*

… …



Invisible Entry Mechanism

… …

- ☆ *Physical block*
- ☆ *Eye tracking*
- ☆ *Tactile sensor*
- ☆ *Pressure sensor*
- ☆ *Vibration sensor*
- ☆ *Back-of-Device interface*

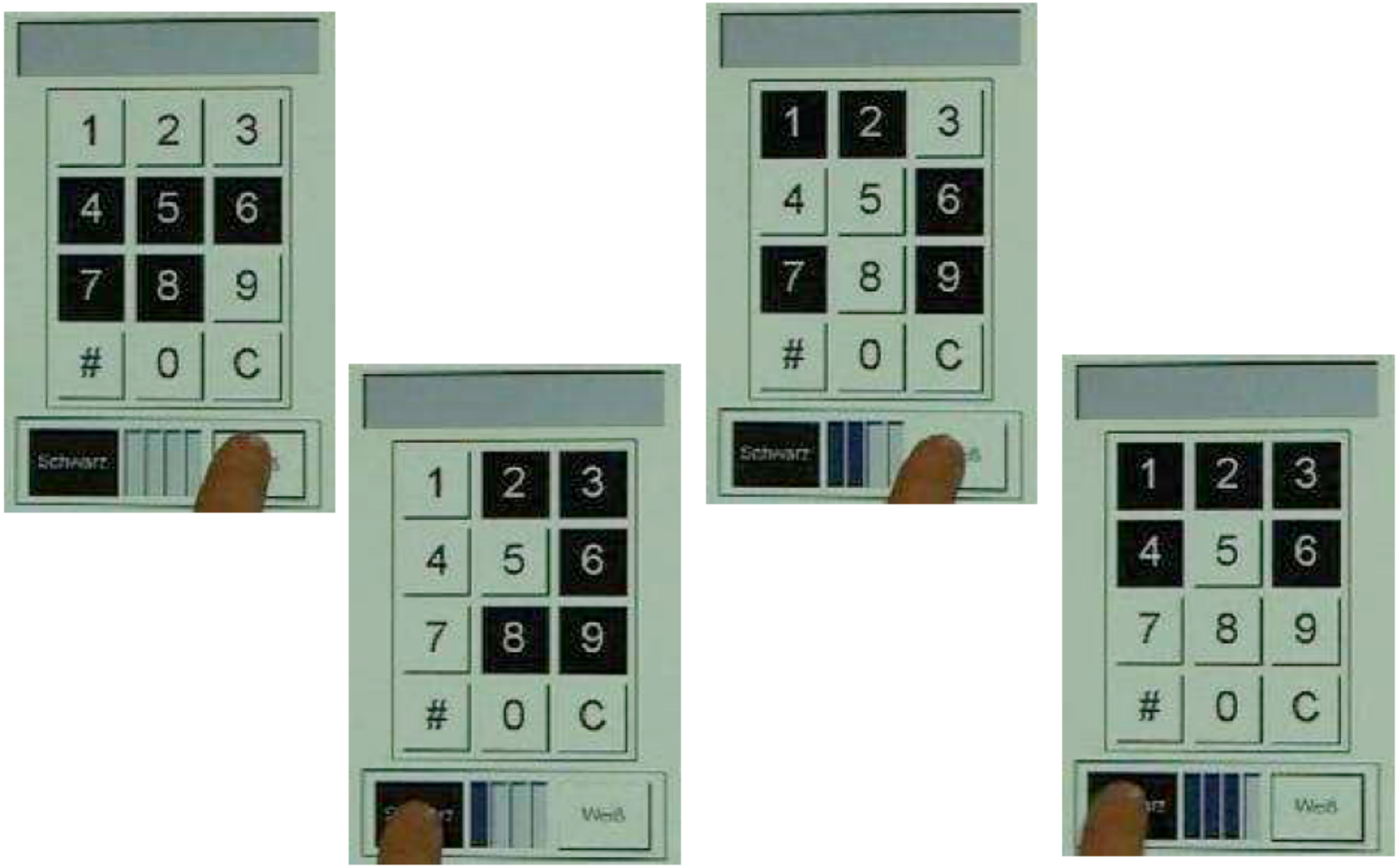
Special human-computer Interface

Hardware support

Deployment costs

SlidePIN

PINEntry



A PINEntry Method Resilient Against Shoulder Surfing@ CCS 2004

ColorPIN

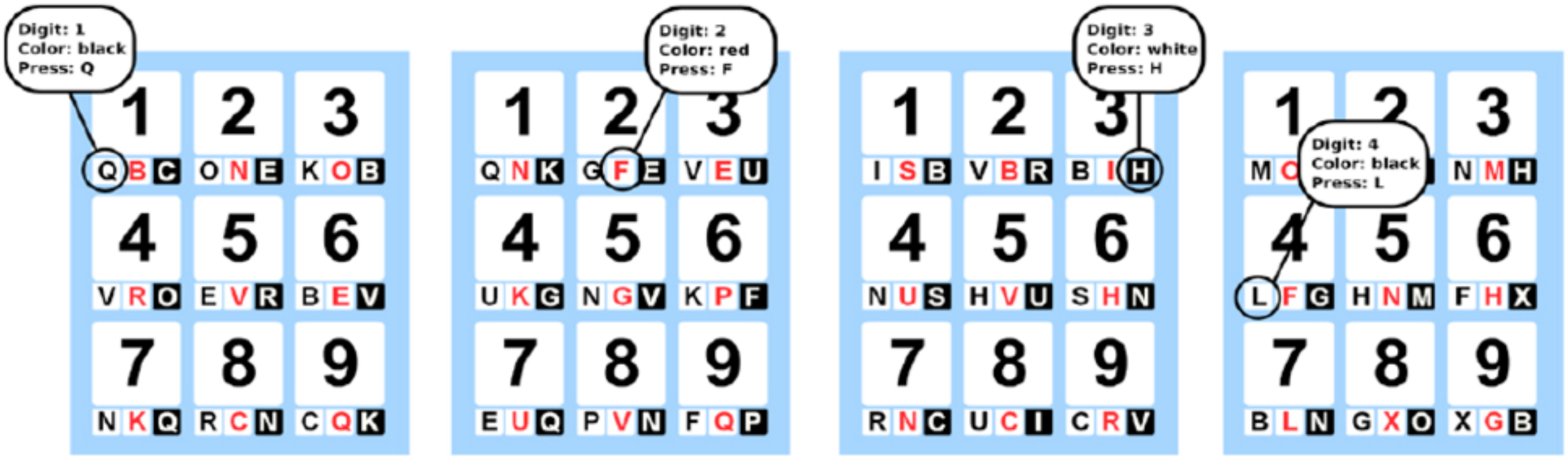


Figure 1: Exemplary PIN entry with ColorPIN. To input the PIN 1(black) 2(red) 3(white) 4(black) the user inputs the letters "QFHL". After each key press, letter assignment changes randomly.

ColorPIN-Securing PIN entry through indirect input @ CHI 2010

BoD AuthE

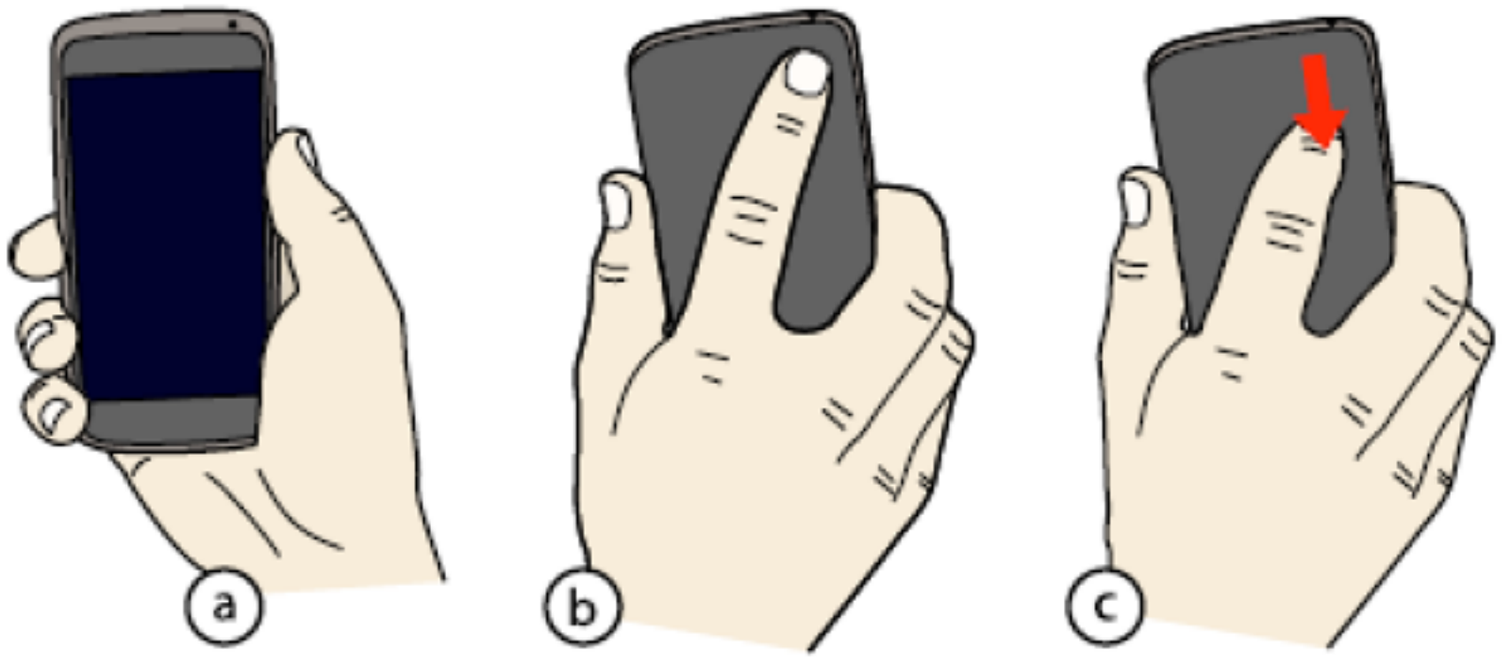
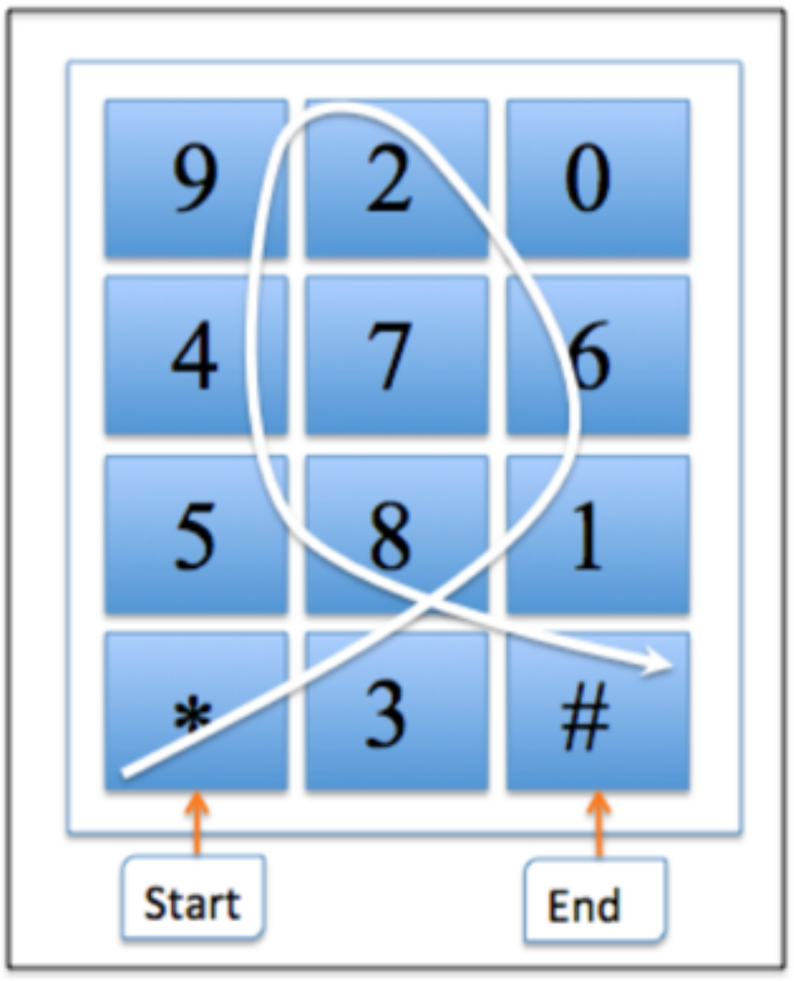


Figure 1. BoD (Back-of-Device) Shapes authentication concept. a) Typical hand posture when using one-handed input for authentication. b) The user authenticates by performing a row of simple shapes on the back. c) Example of a user performing a single-stroke shape ("Down").

Back-of-Device Authentication on Smartphones @ CHI 2013

SlidePIN概念

Slide-based PIN Entry Mechanism



Random Keypad

Slide

Input with random numeric keypad is more secure

Word-Gesture Keyboard

PIN 1245

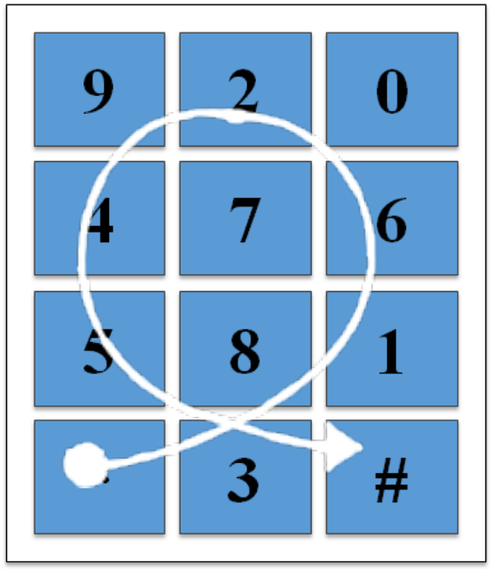
SlidePIN *381629458#

Slide input is faster

Slide input is more secure

模型分析

PIN: 1245

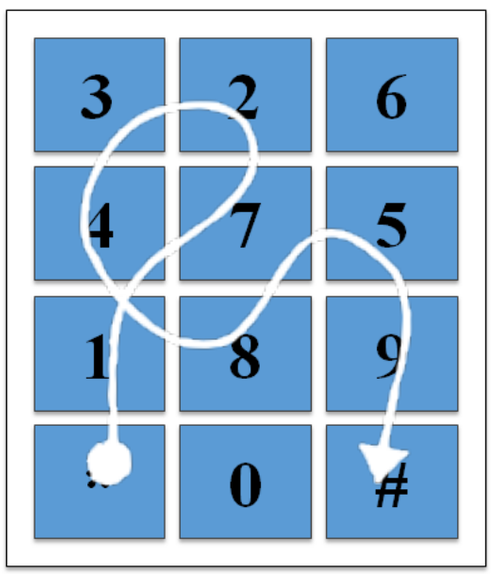


Layout 1

Trajectory 1

Sequence 1

*381629458#



Layout 2

Trajectory 2

Sequence 2

*147234185 9#

Slide Map Function

F (PIN, Layout) → Sequence

Attack Function

One-Time

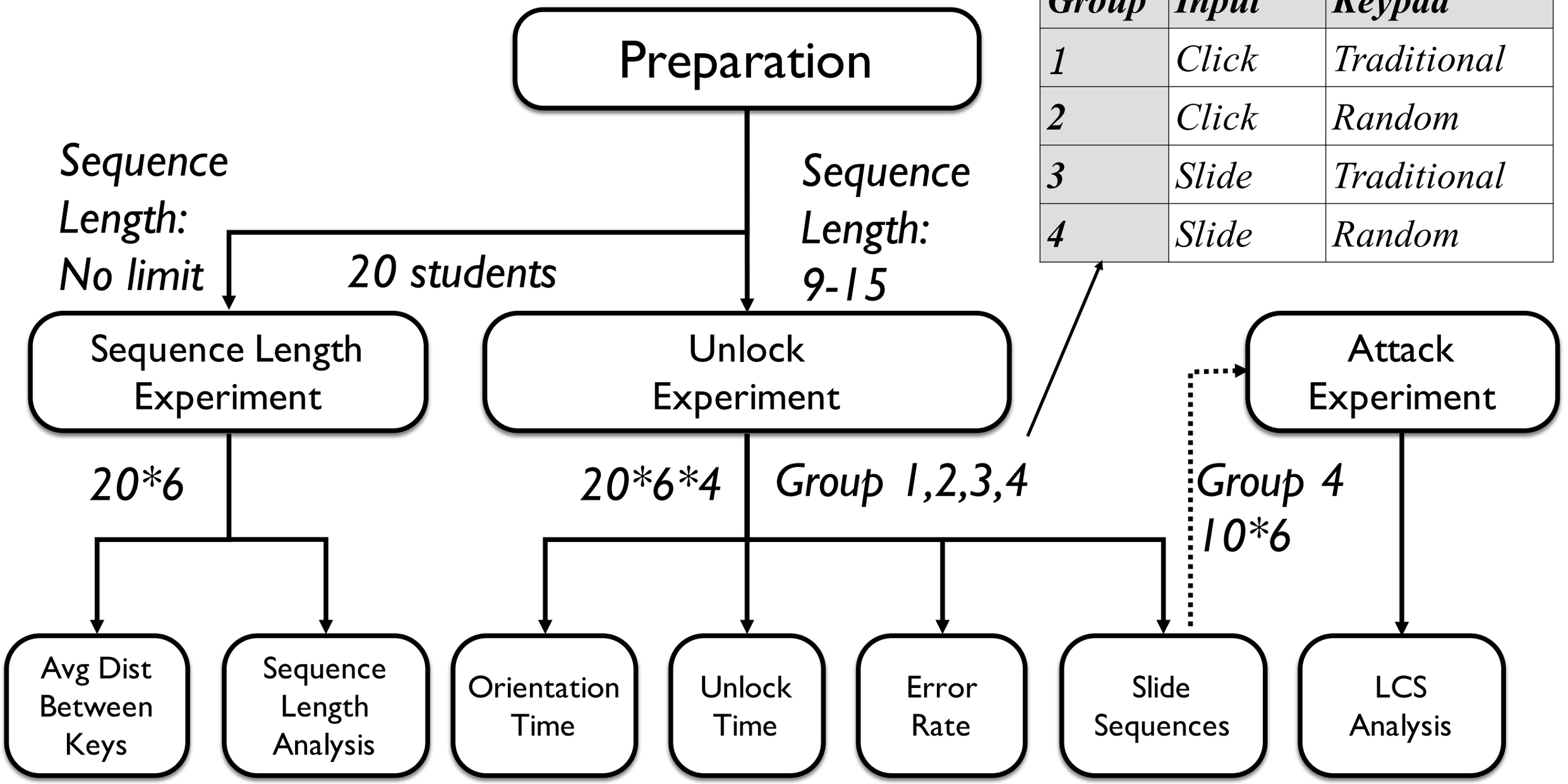
F^{-1}(Sequence 1) → PIN

Multi-Time

F^{-1}(Sequence 1,
Sequence 2,
… …
Sequence n) → PIN

实验设计

Group	*Input*	*Keypad*
1	*Click*	*Traditional*
2	*Click*	*Random*
3	*Slide*	*Traditional*
4	*Slide*	*Random*



序列长度分析

Too long * 0123456789 0123456789 0123456789 0123456789 #

Why

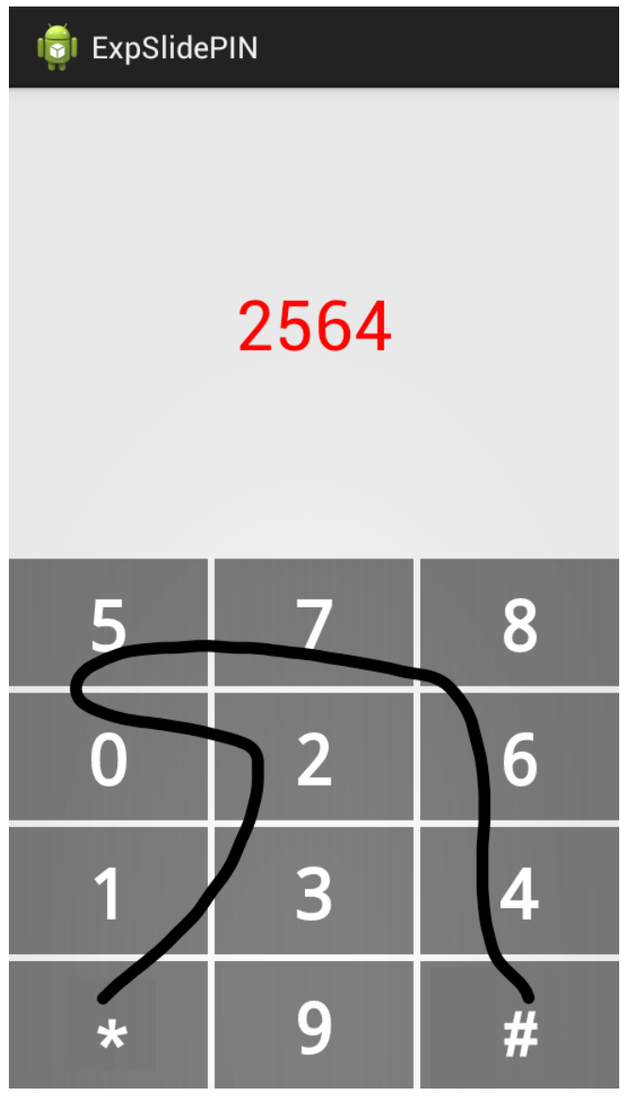
*3816279450#

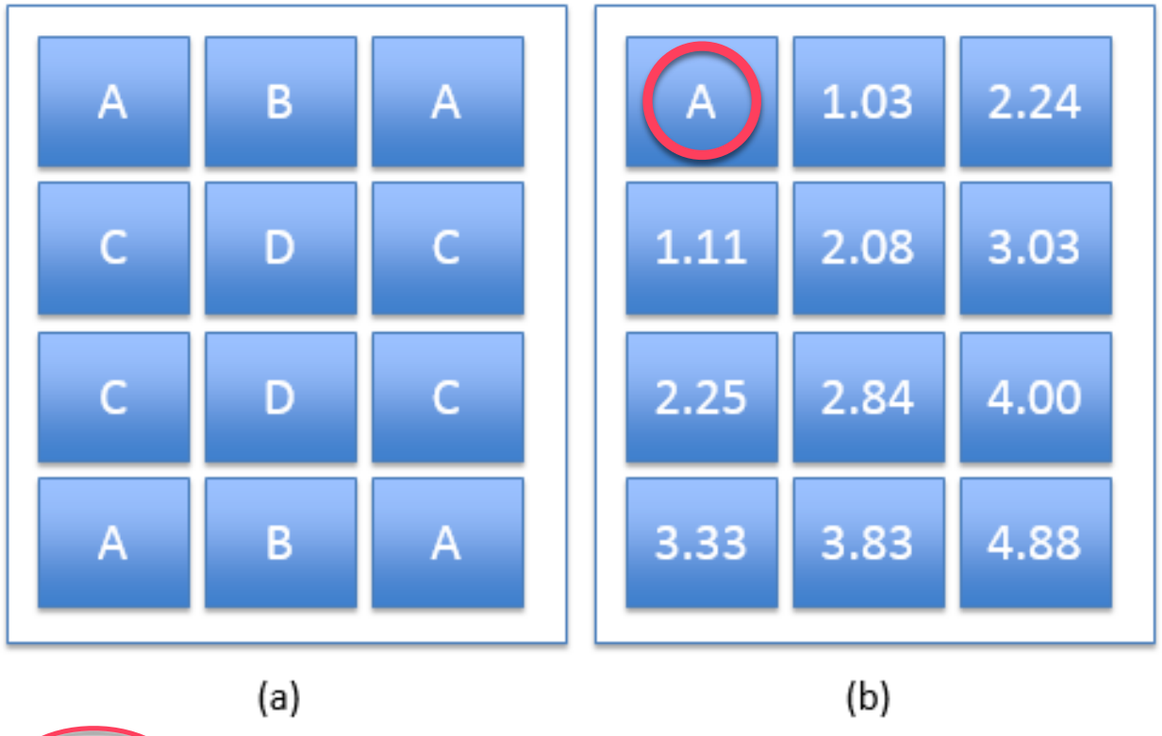
*381629450#

Too short *31629450#

How

20 students
** 6 times*





Estimate of Distance between Keys

$D(A)=(1.03+2.24+1.11+2.08+3.03+2.25+2.84+4.00+3.33+3.83+4.88)/11\approx 2.78$

序列长度分析

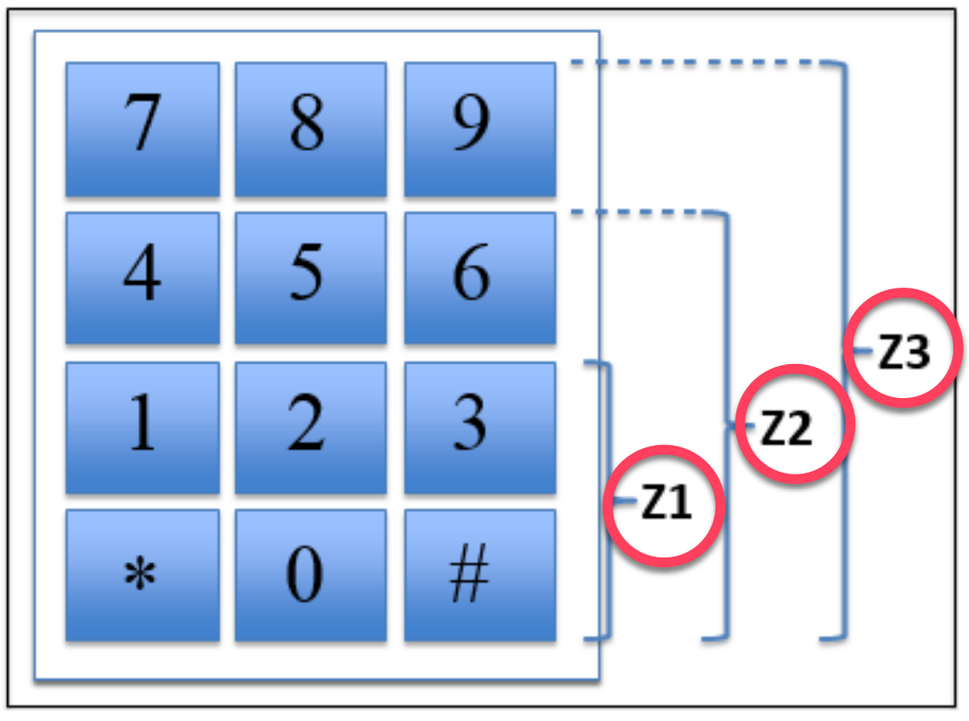
(a) (b) (c)

$D(B) = 2.38$

$D(C) = 2.25$

$D(D) = 1.87$

$Davg = (D(A)*2+D(B)*2)+D(C)*4+D(D)*2) / 10 \approx 2.31$



$P(Z3) = 1$ $D(Z3) = 11.55$

$P(Z2) = 1/6$ $D(Z2) = 10.82$

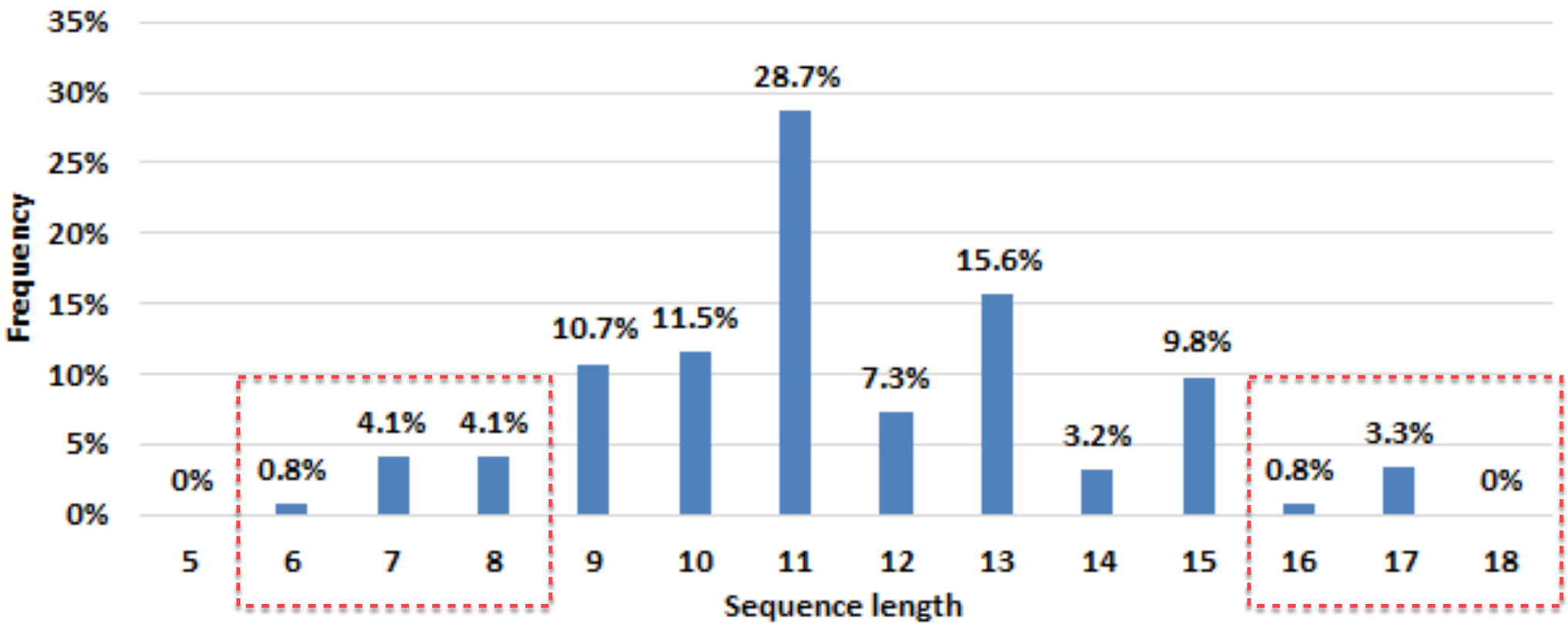
$P(Z1) = 1/200$ $D(Z1) = 8.08$

$8.08 * 1.87 \approx 15.11$

9 - 15

序列长度分析

- *Estimate of Sequence Length*
  - ✴ *Mean value of sequence length: 11.55 vs 11.46*
  - ✴ *Lower threshold of sequence length: 9*
  - ✴ *Upper threshold of sequence length: 15*



安全性分析

- *Shoulder surfing attack*

One-Time

Sequence Length	*9*	*10*	*11*	*12*	*13*	*14*	*15*
PIN	*126*	*210*	*330*	*495*	*715*	*1001*	*1365*

Multi-Time

Times	*u1*	*u2*	*u3*	*u4*	*u5*	*u6*	*u7*	*u8*	*u9*	*u10*
2	*6*	*6*	*6*	*6*	*7*	*6*	*6*	*7*	*6*	*4*
3	*5*	*5*	*4*	*4*	*4*	*4*	*4*	*5*	*4*	
4	*4*	*4*						*4*		

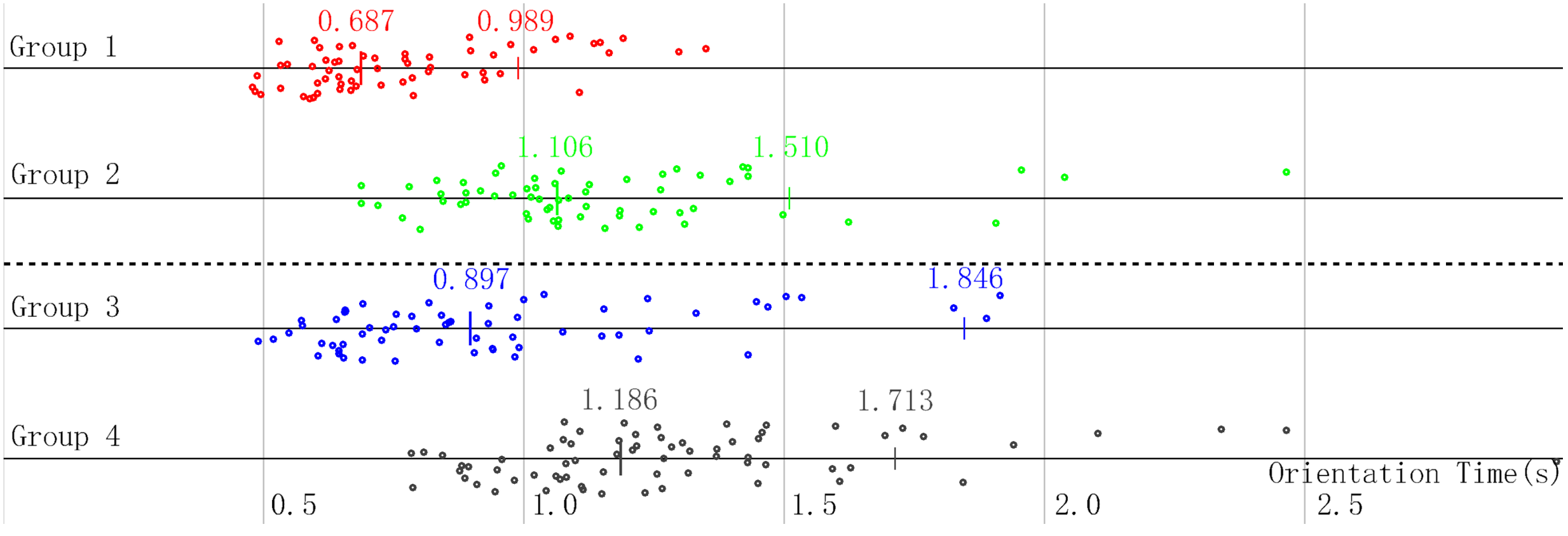
- *Guessing attack*
  - ✴ *Brute force attack*
  - ✴ *Dictionary attack*

- *Replay attack*
  - ✴ *Random numeric keypad*

可用性分析

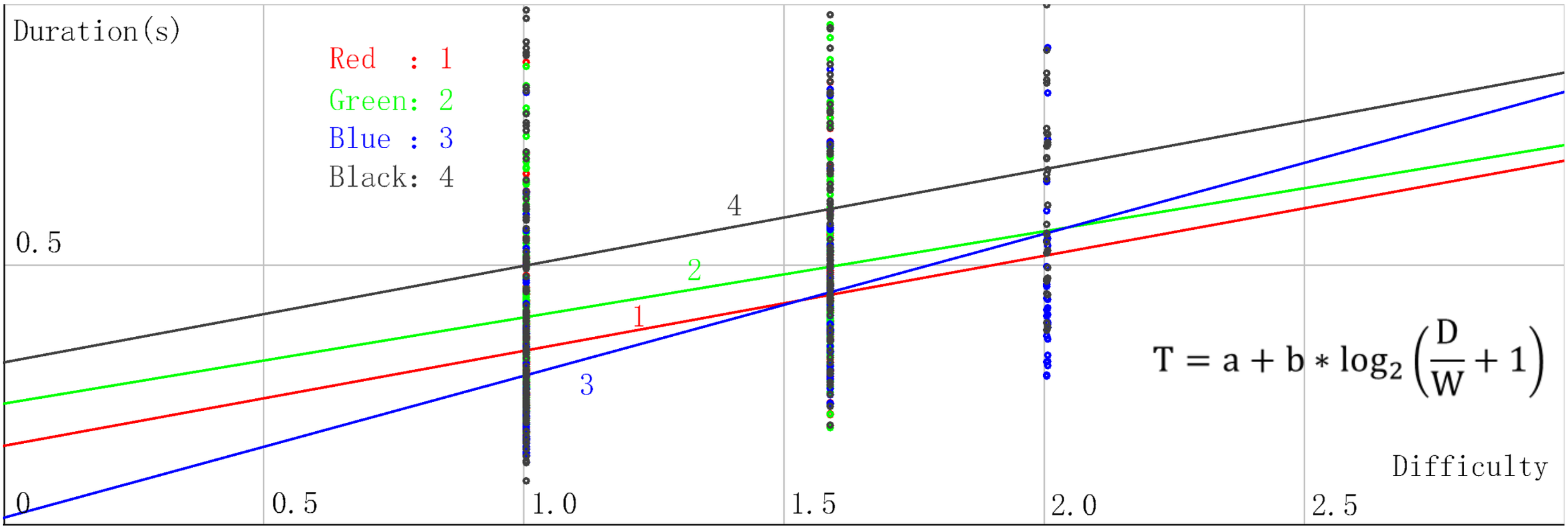
- *Orientation time*

Groups	*Average*	*Standard Deviation*	*Threshold Value*
1	*0.687*	*0.133*	*0.989*
2	*1.064*	*0.199*	*1.510*
3	*0.798*	*0.293*	*1.846*
4	*1.186*	*0.225*	*1.713*



可用性分析

- *Unlock time*
  - ✴ *Sliding is faster*
  - ✴ *Input sequences become longer*
  - ✴ *Random number keypad increases unlock time*



可用性分析

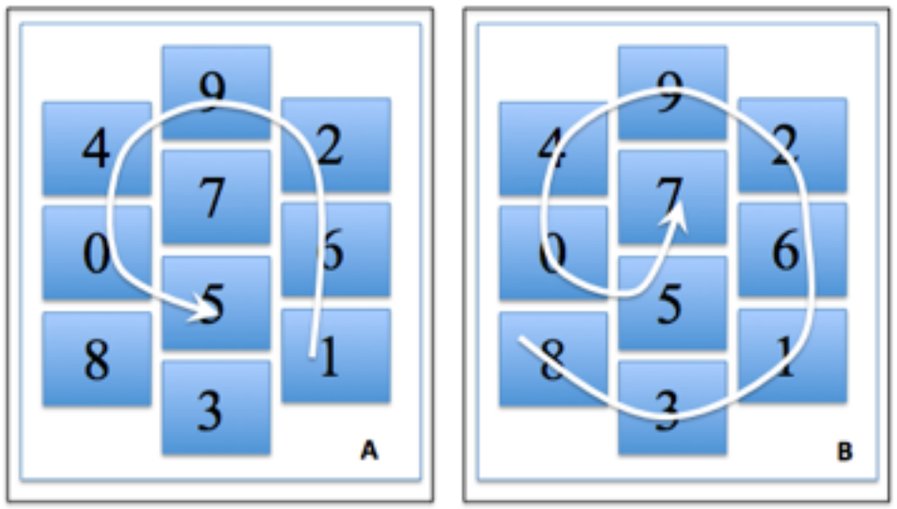
- Error rate
  - ✴ *Sequence length limit*
  - ✴ *Start point and end point*
  - ✴ *Not familiar enough*

Groups	*Error Rate*
1	*1.67%*
2	*3.33%*
3	*7.69%*
4	*13.04%*

- Cost of learning
  - ✴ *SlidePIN is built based on 4-digits PIN*
  - ✴ *SlidePIN is easy to use*
  - ✴ *SlidePIN is interesting to use*

SlidePIN

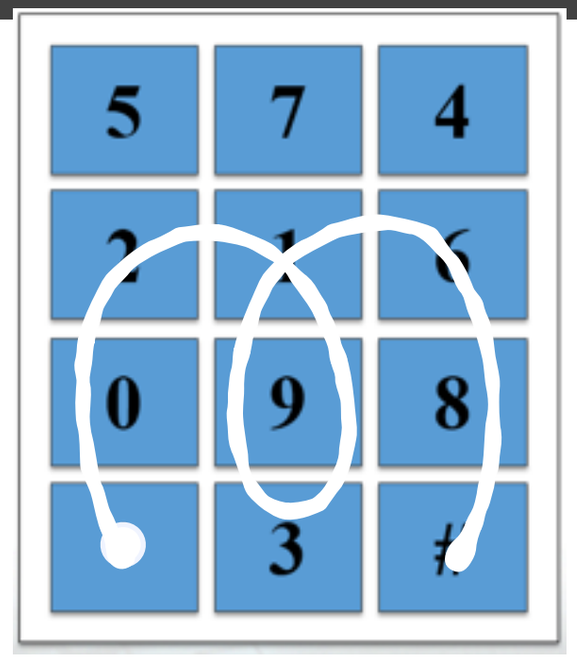
讨论



PIN: 1245

PIN: 2118

*021939168#



1: Fixed start point and end point

2: Same adjacent Digits

3: PIN storage

Device ID or SIM ID

↓

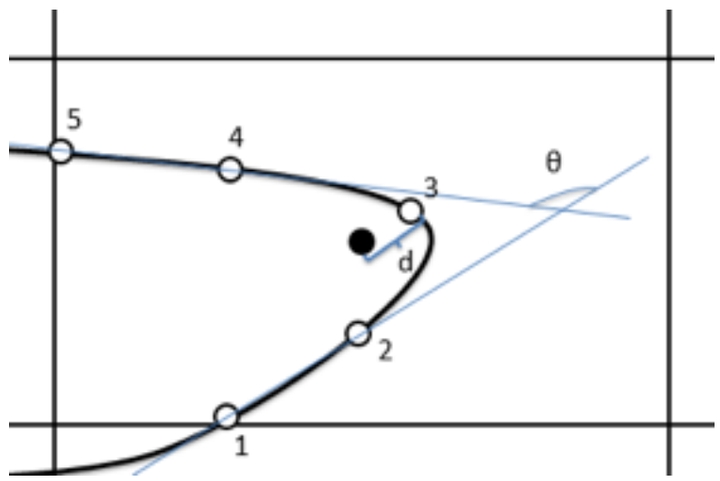
Key

↓ encrypt

PIN

4: Smudge attack

5: Attack based on Features



谢谢！

孙惠平

sunhp@ss.pku.edu.cn