

# *Information Security Engineering*

2017.09.27

## 图形口令



*Huiping Sun(孙惠平)*  
[sunhp@ss.pku.edu.cn](mailto:sunhp@ss.pku.edu.cn)

# 课程项目

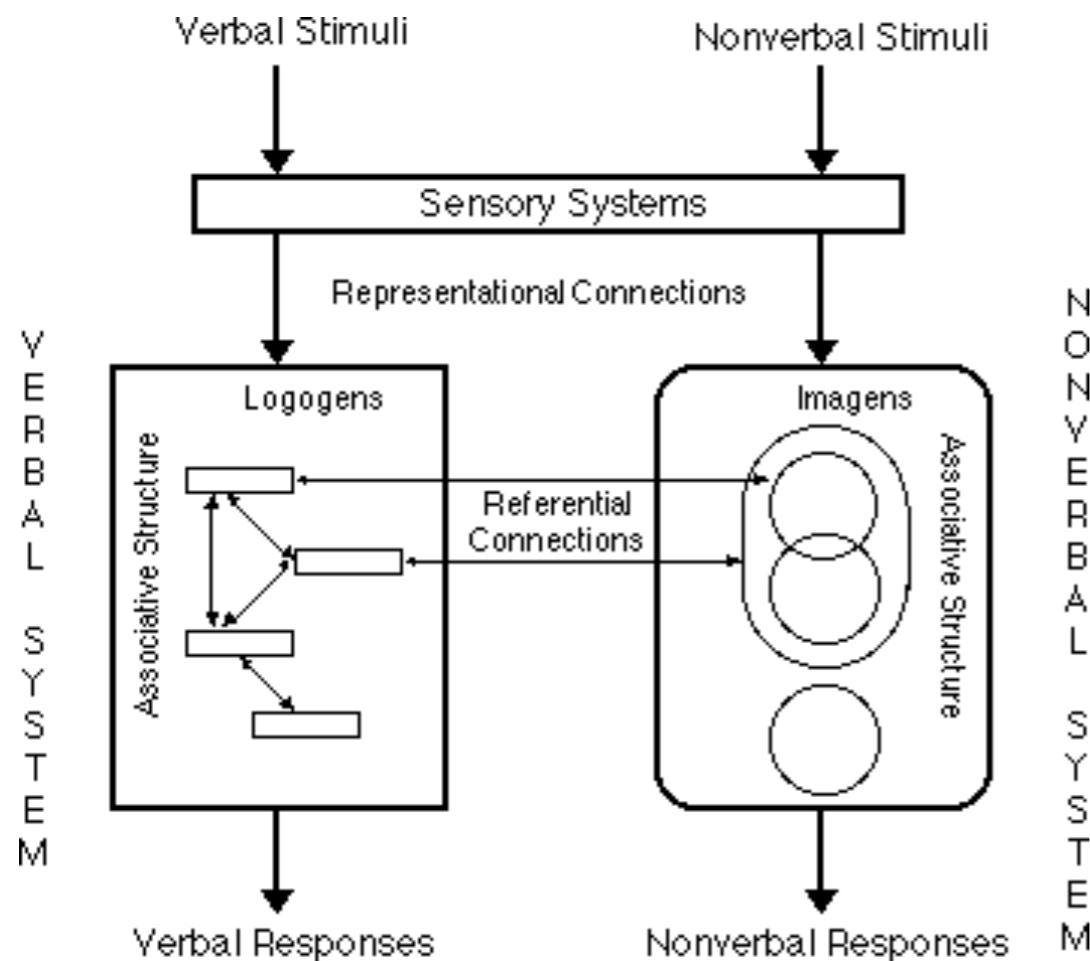
- 自由组队，**3-4人**，**10月10日前**确定组队和选题；
- 选择一个和课程相关的**安全产品**作为对标，设计实现一个类似产品；
- 需要提交产品调研报告、论文阅读笔记、论文总结报告、设计报告、代码等；
- 每个人需要注册一个**github账号**，所交材料需要上传github；
- 考核主要看选择**题目的难度和完成的质量**，最后一次课进行项目汇报；
- 选题参见昨天课程微信群发的txt文件，有问题可以随时联系我，如需要可以约时间见面交流；

# 课程内容

- 图形口令简介
- 图形口令分类
- 例子： PassApp
- 图形口令评价

# 图形口令

使用图形作为口令构成元素



**Dual Coding Theory**

- Recall
- Recognition
- Cued Recall

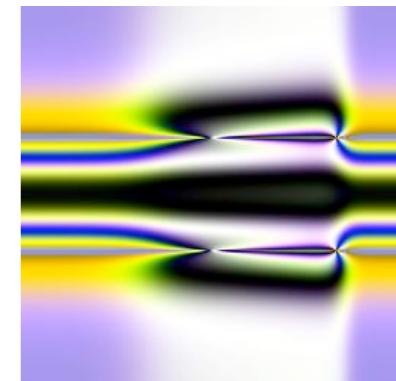
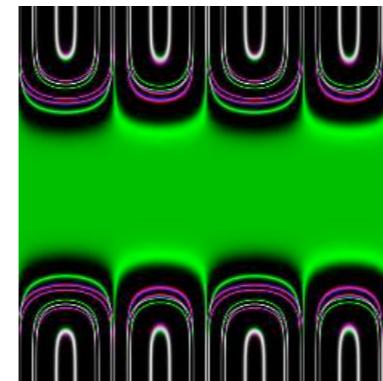
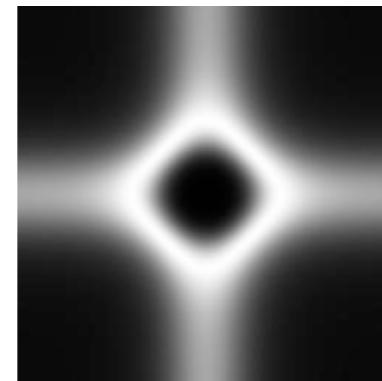
*Recognition is an easier memory task than recall*

*With the aid of a retrieval cue, more information can be retrieved*

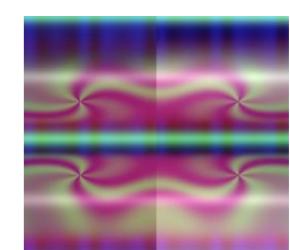
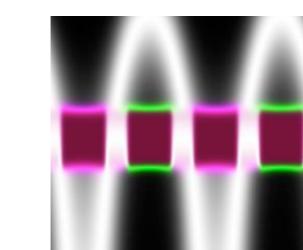
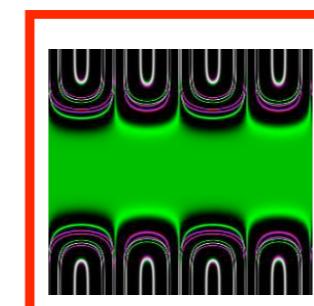
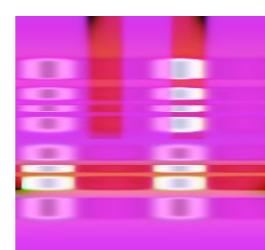
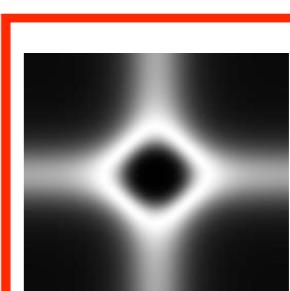
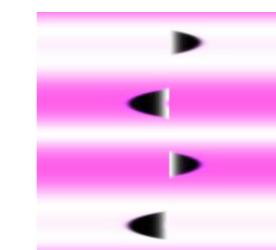
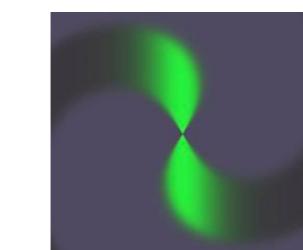
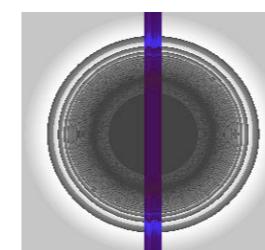
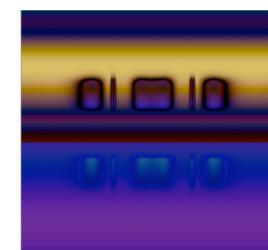
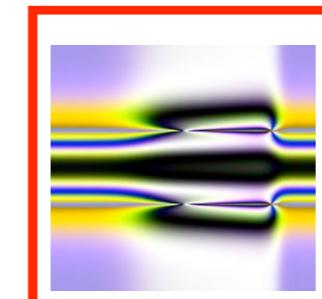
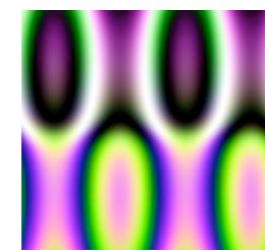
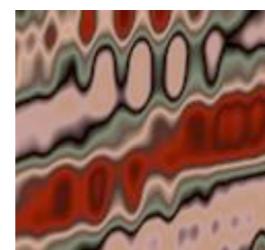
# *Introduction*

# Déjà Vu

训练



挑战



# PassFaces

- 系统从脸型数据库中随机选取5个人的脸型，显示给用户，并给用户一定时间让用户熟悉（注册）
- 系统每次显示9个脸型（其中仅有一个是注册时显示给用户的）让用户选择，这样的选择共进行5次
- 如果用户正确的选择了所有的5个脸型，用户身份认证成功，否则失败（登入）



## Introduction

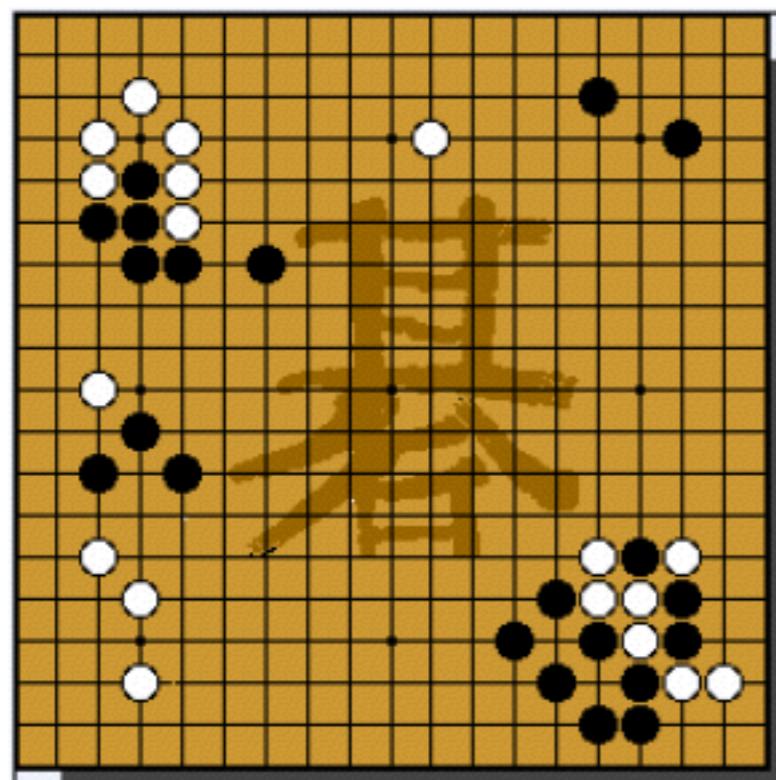


Figure 1 Go game

## Pass-Go

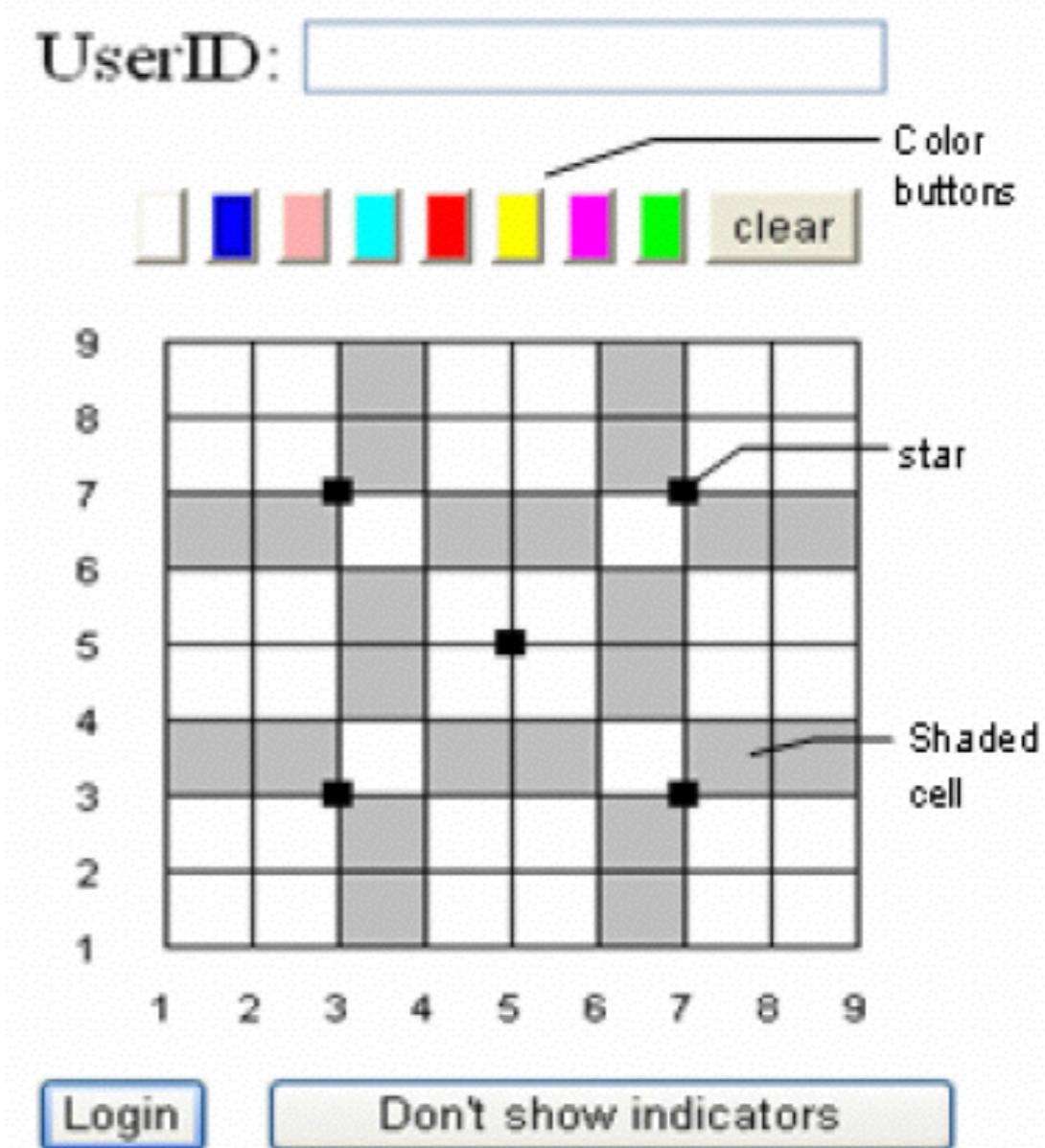
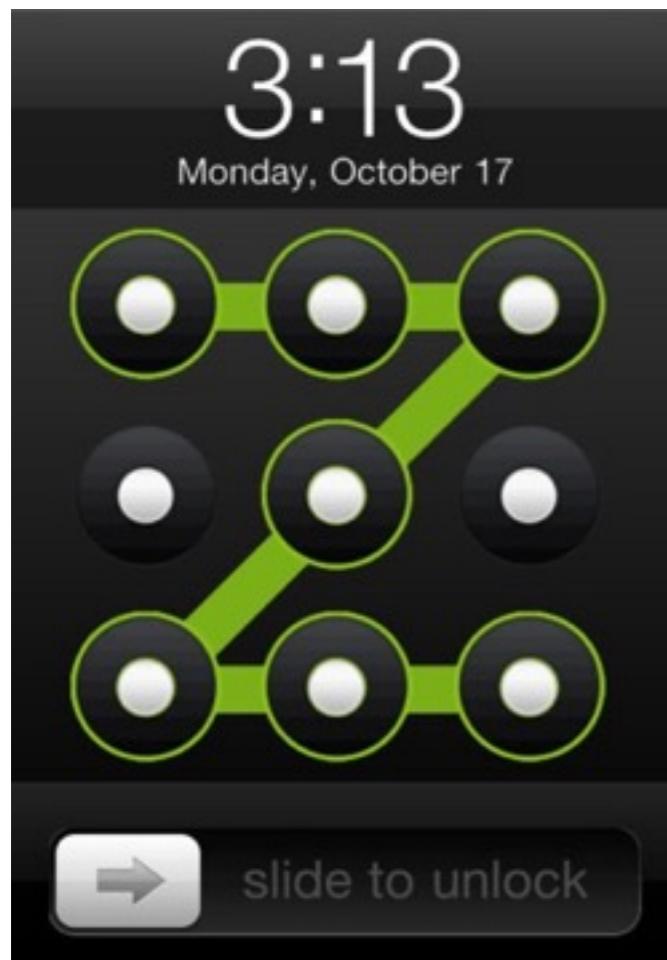


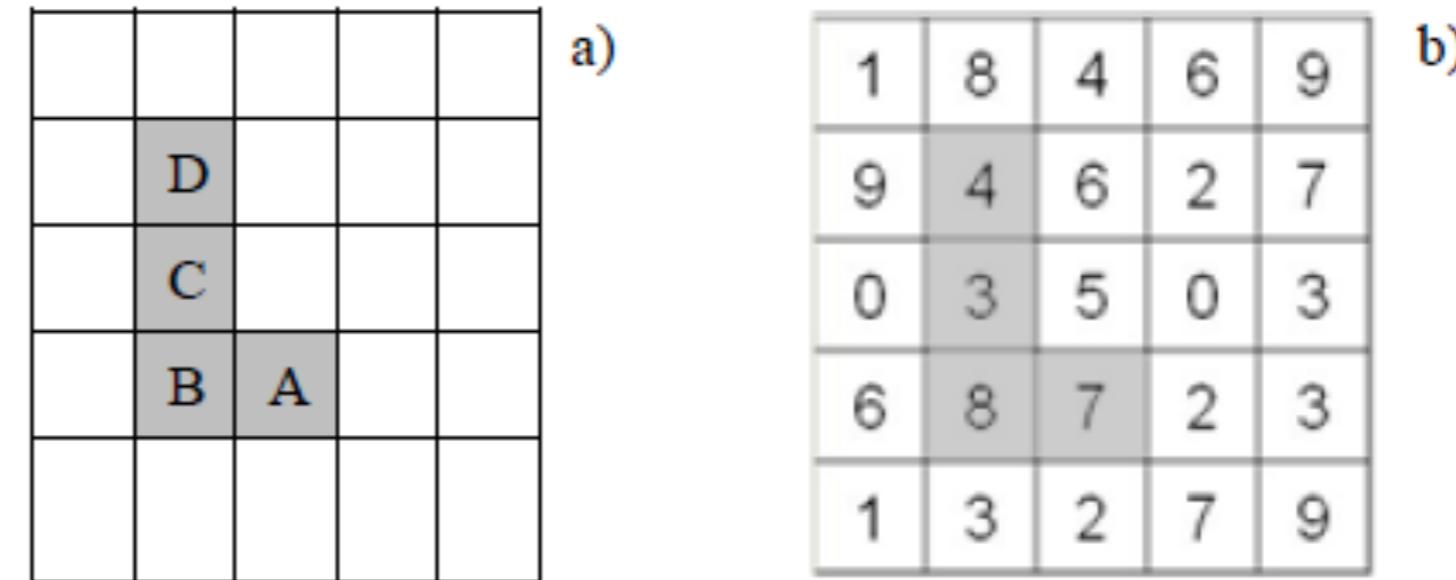
Figure 22 Main login interface

# Introduction

## 商业产品



**PatternLock**



**Figure 1. a)** Enrolling in the system. User picks cells A, B, C and D.

**b)** Authenticating with the system. User reads off random numbers chosen cells.

**GrIDSure**

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

(a)  $k = 4$

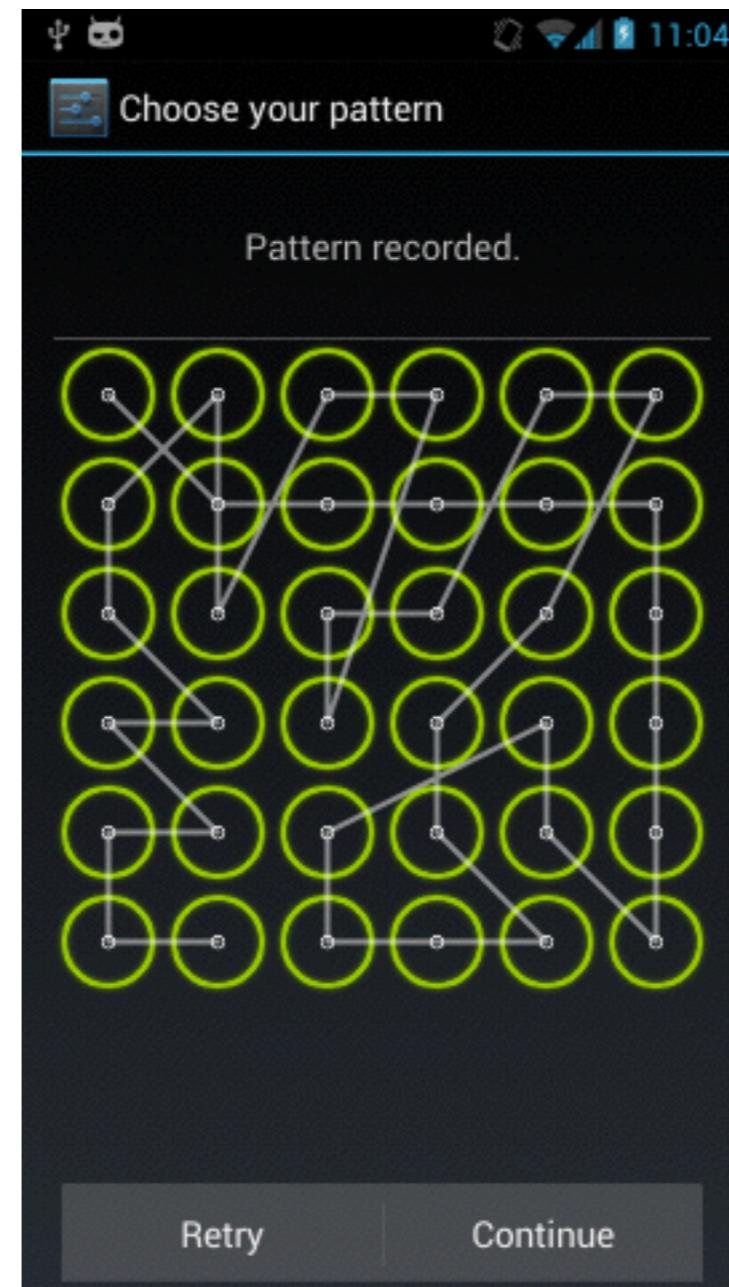
1	8	3	8	2	0	4	5	8
7	1	9	5	2	5	9	3	0
5	4	7	7	4	6	2	7	3
3	5	0	6	4	7	1	0	3
2	4	6	8	5	1	2	6	9
8	1	4	3	9	2	6	4	5
7	5	6	8	9	4	2	1	9
4	7	0	5	8	2	8	9	6
1	2	3	3	7	6	3	5	0
8	2	7	5	0	1			
4	9	3	4	9	3			

(b)  $k = 8$

**GridCode**

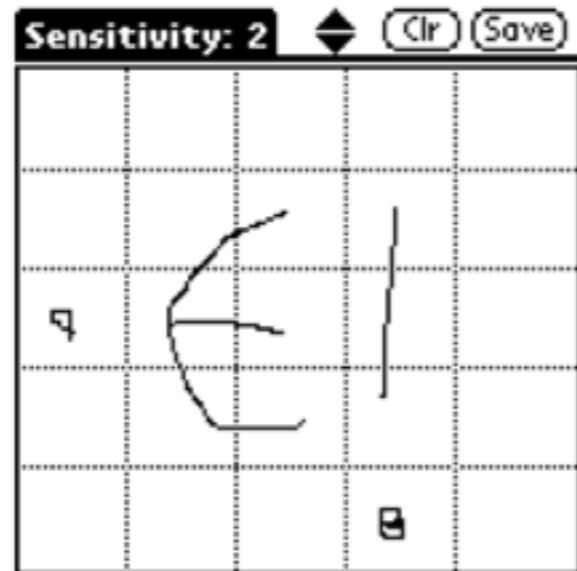
## Introduction

# Pattern Lock

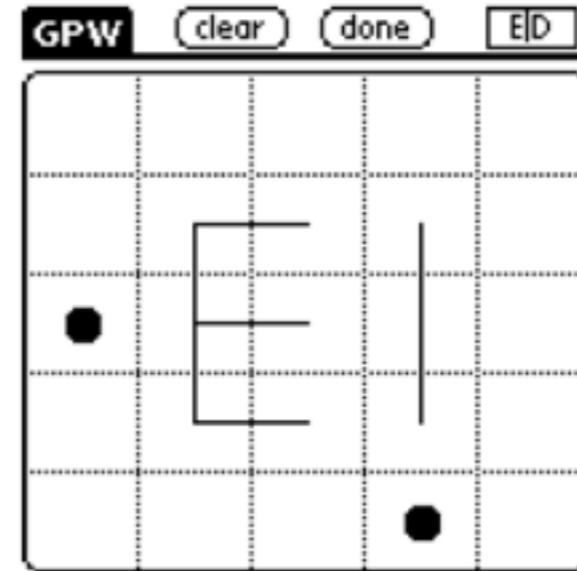


基于  
回忆、识别、线索回忆  
的图形口令

对称图像  
很少笔画  
中心放置



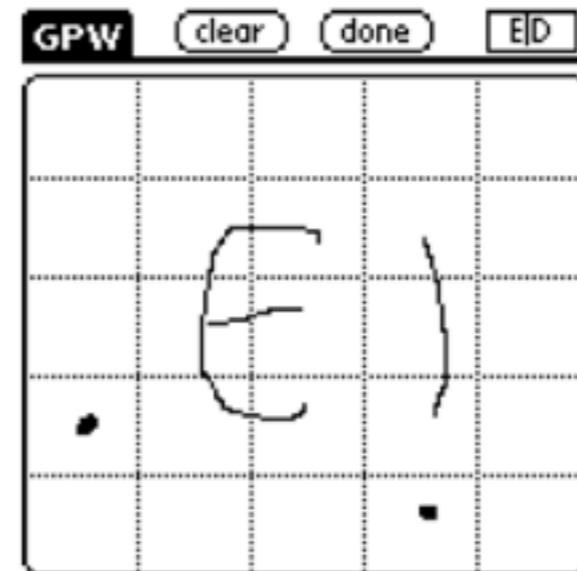
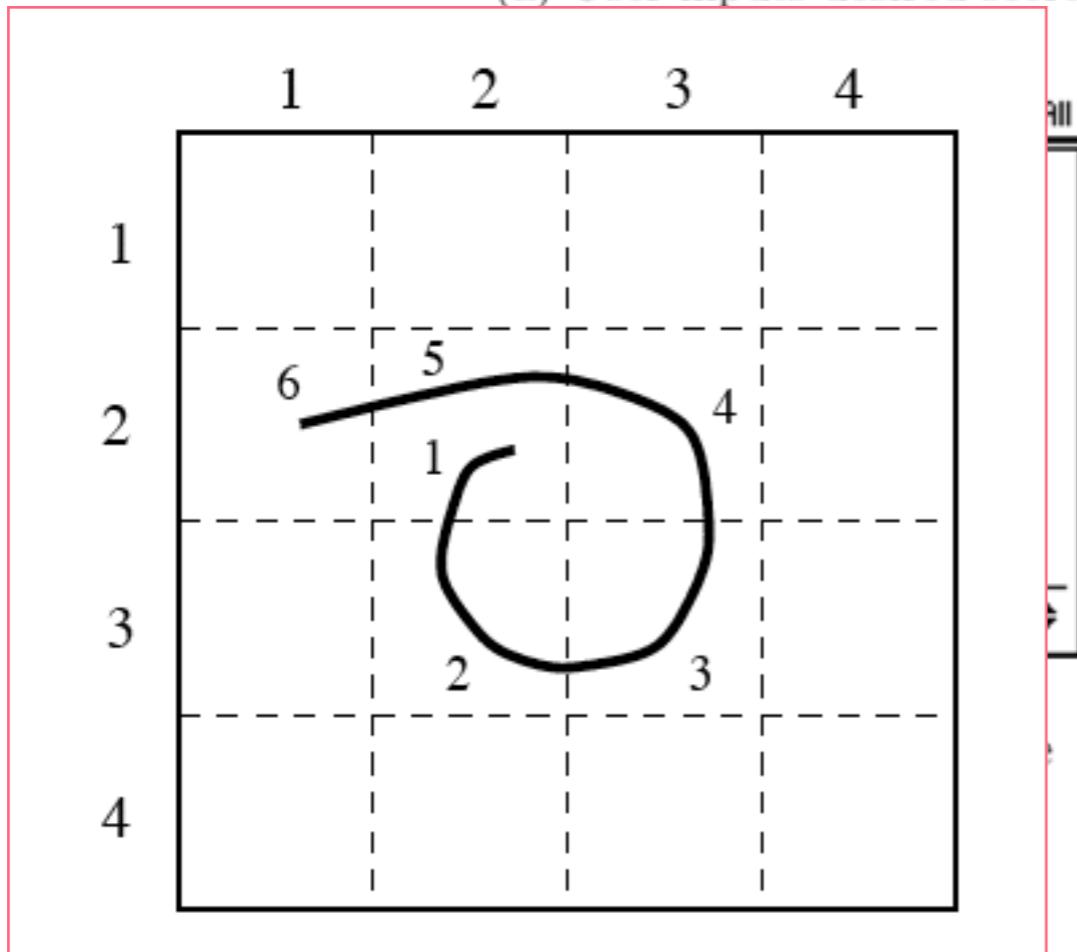
(a) User inputs desired secret



(b) Internal representation



(c) Raw bit string

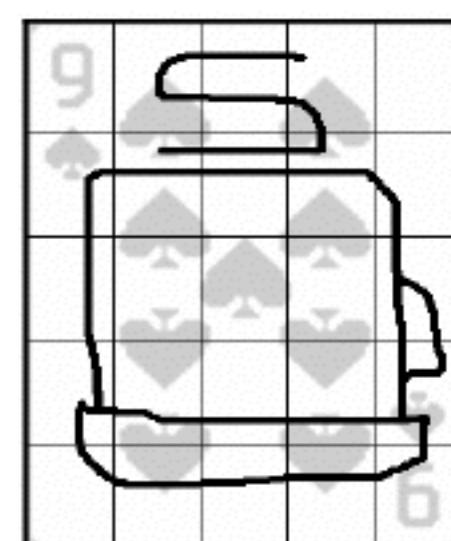
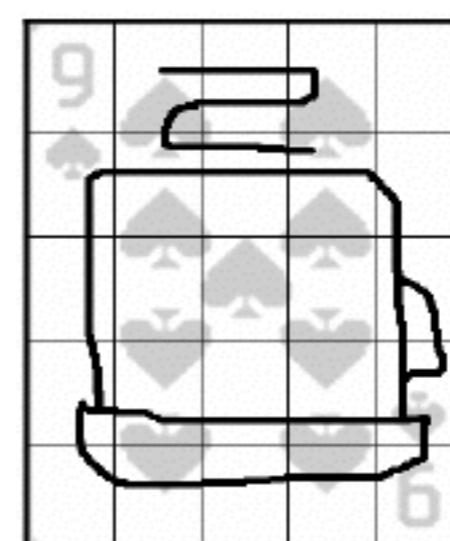
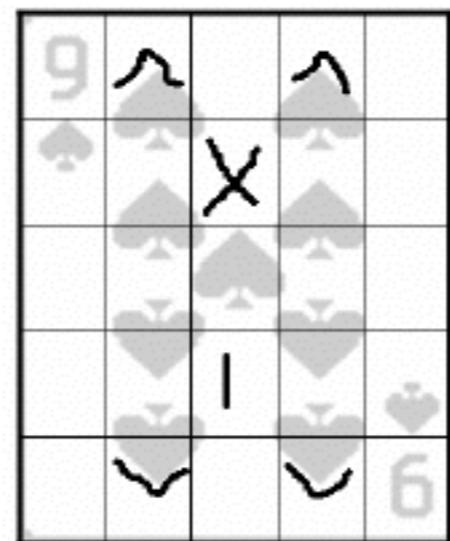
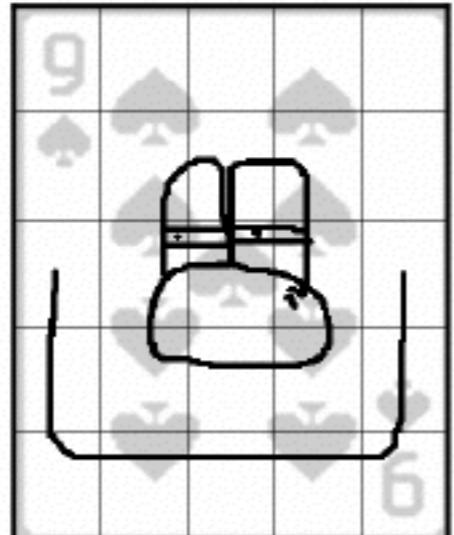
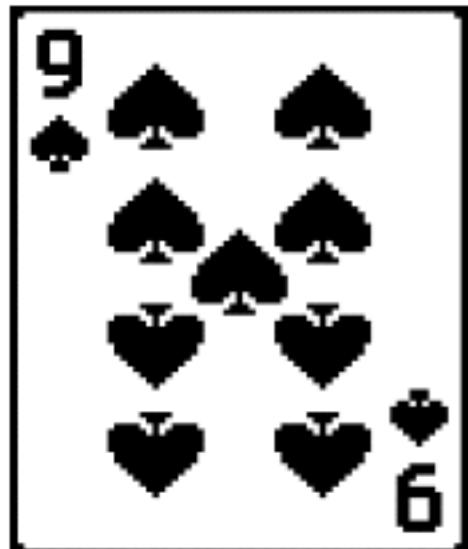


(e) Re-entry of (incorrect) secret



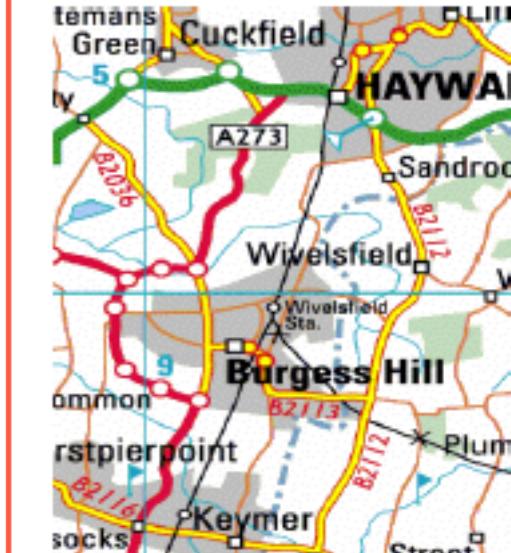
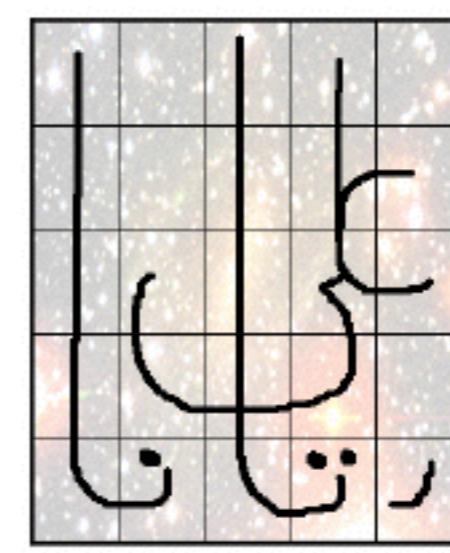
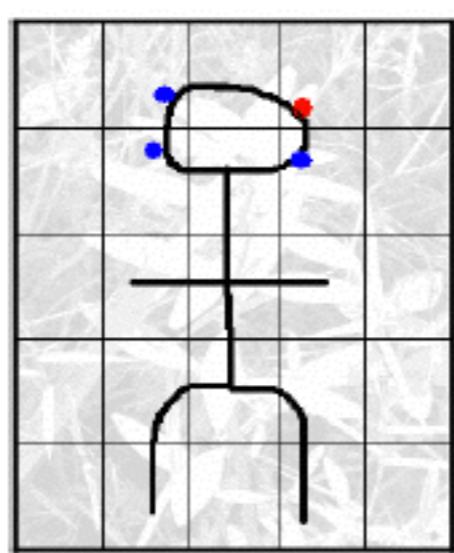
(f) Authorization failed

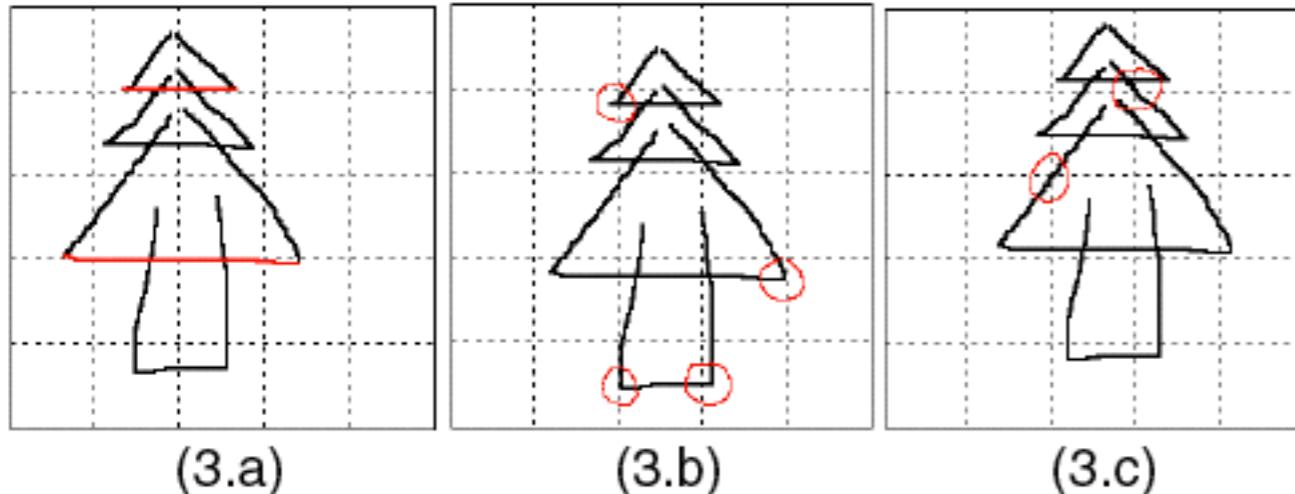
## BDAS: Background DAS



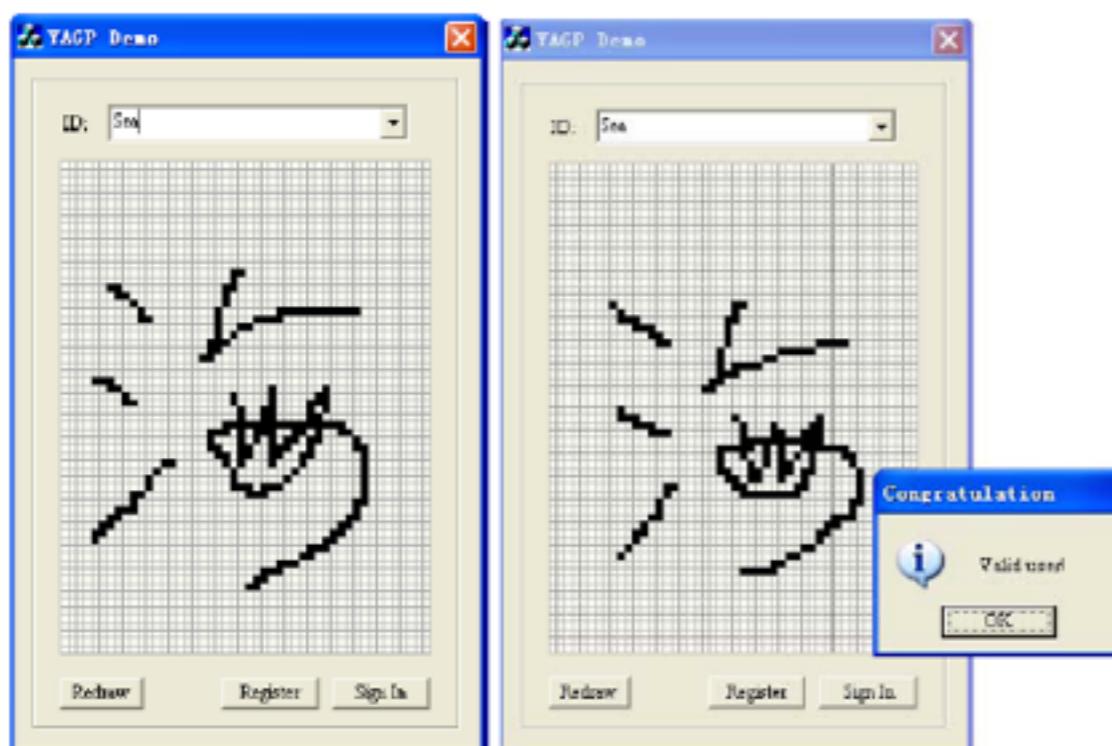
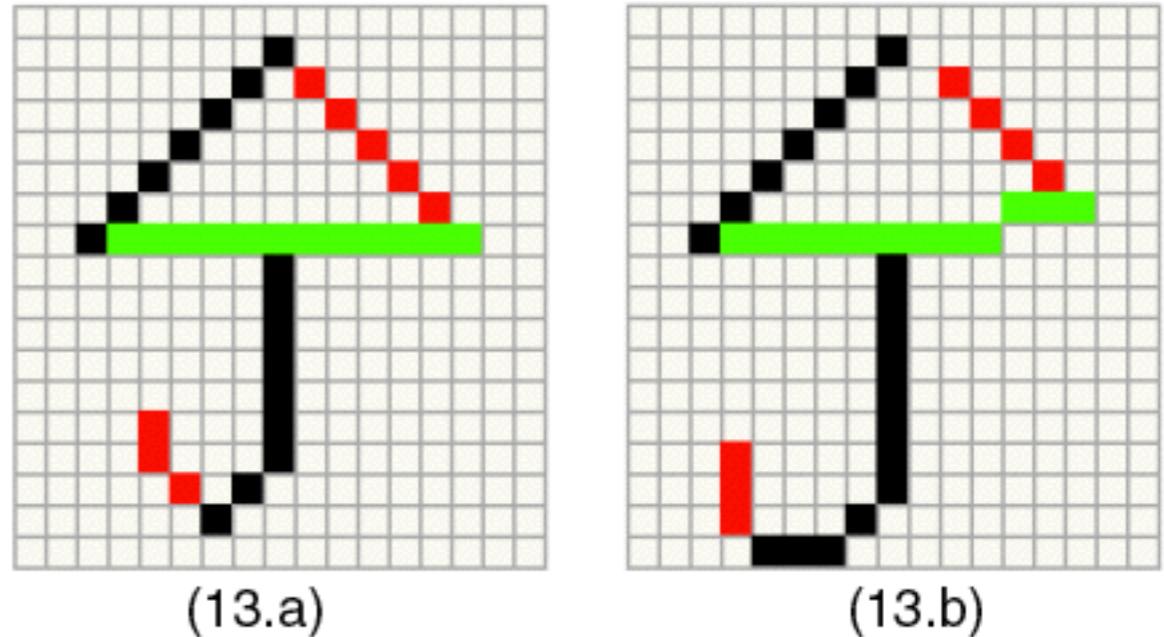
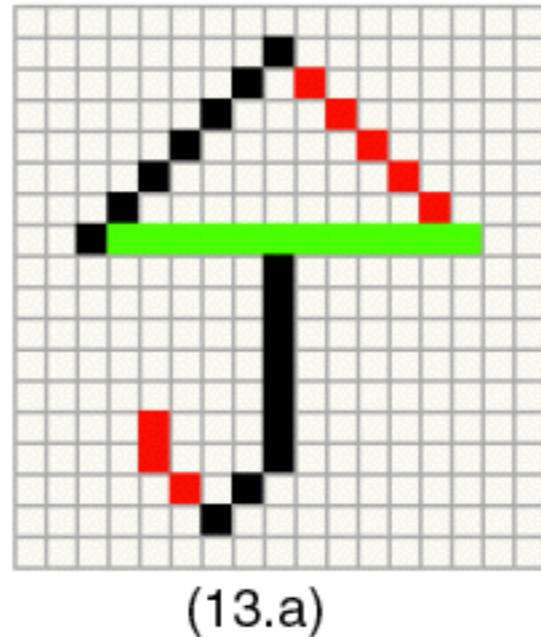
(a)

(b)

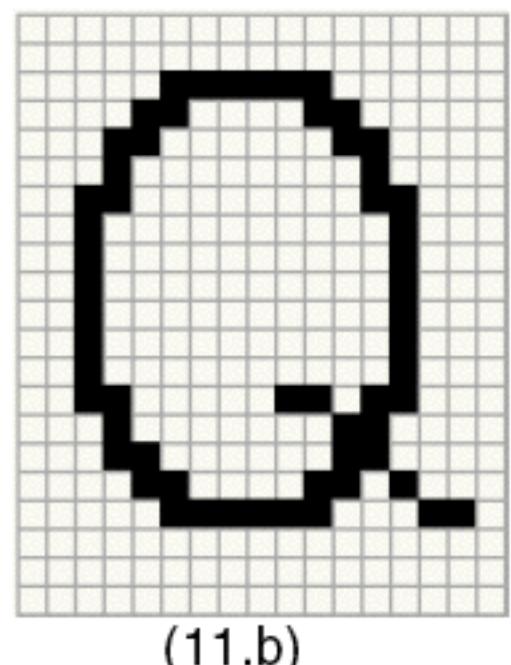
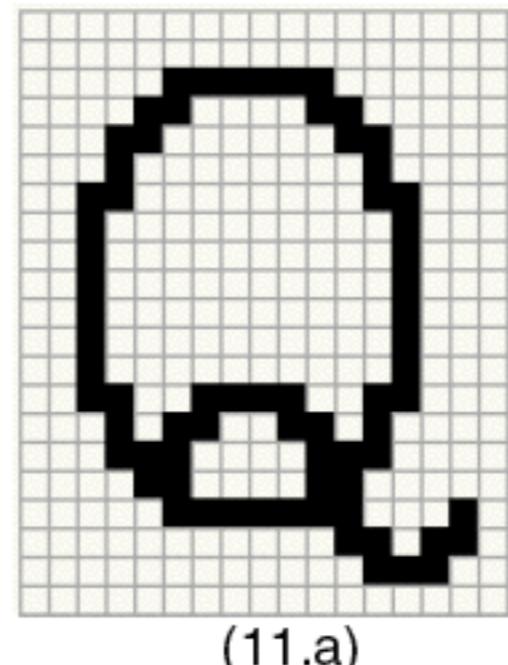


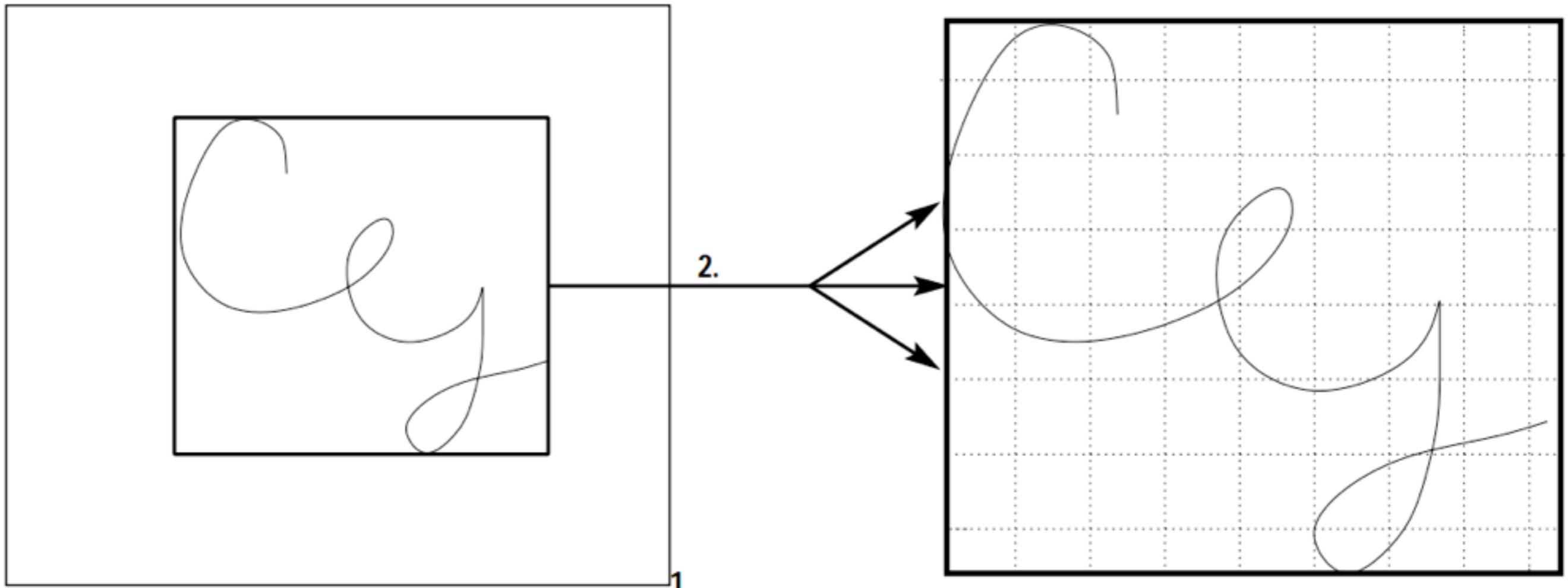


**Figure 3. Examples of rule violations in DAS.  
(a) Lines near grid line. (b) Endpoints near  
grid line. (c) Strokes near cell corner.**



**Figure 15. The YAGP system Interface (48x64  
density grid).**





1. Read mouse input
2. Scale and stretch doodle to grid
3. Analyze against stored user data
  - Compare against distribution grid
  - Measure variance of points across distribution grid
  - Compare instantaneous speed
4. If tests confirm identity of user, authenticate, if not repeat analysis against other stored users.

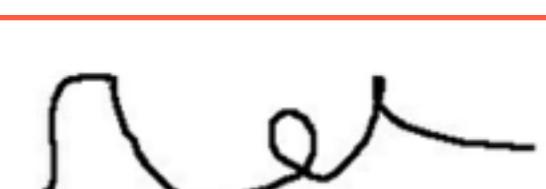
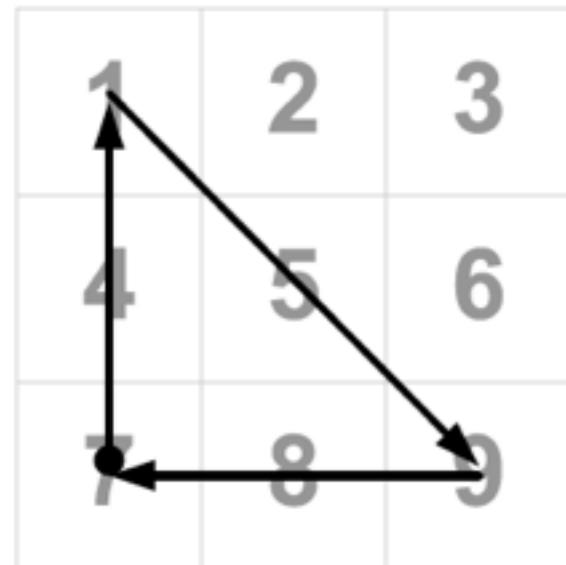


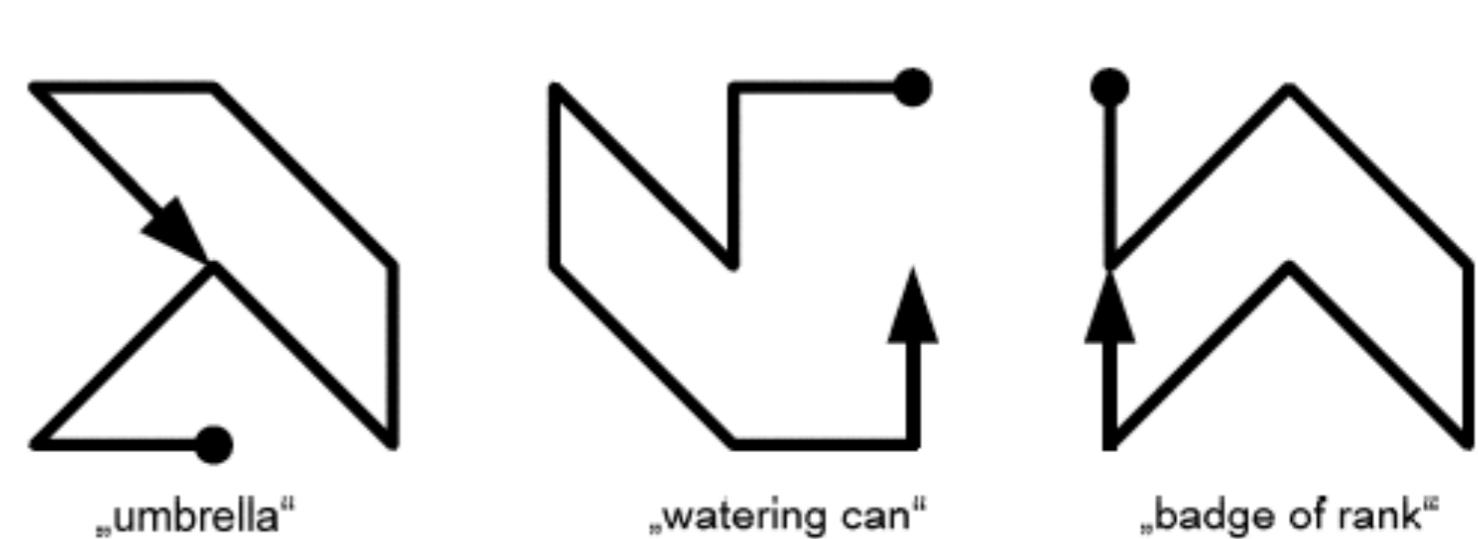
Figure 1: An Example of a Passdoodle

## Recall-Based

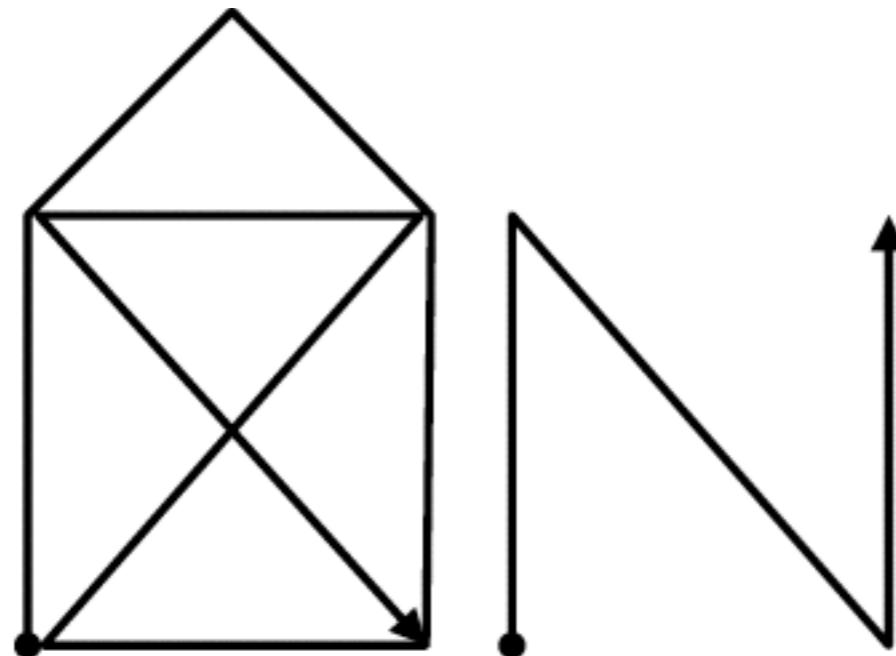
## PassShapes



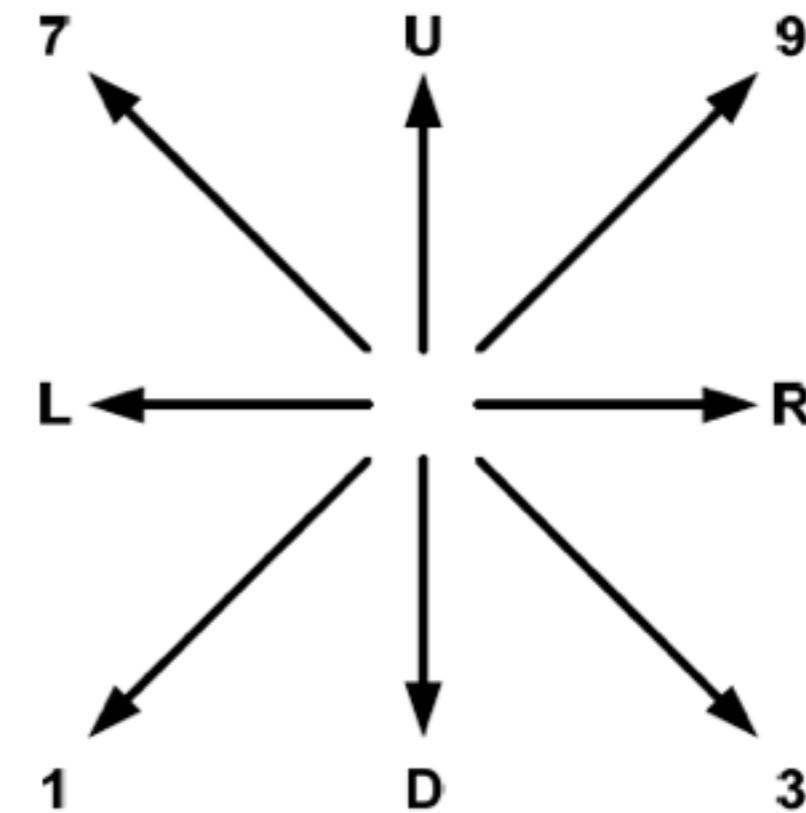
0



**Figure 6: PassShapes and users' associations**



**Figure 3: An example PassShape with the internal representation U93DL9L3XU3U**



# Recall-Based

# Pass-Go

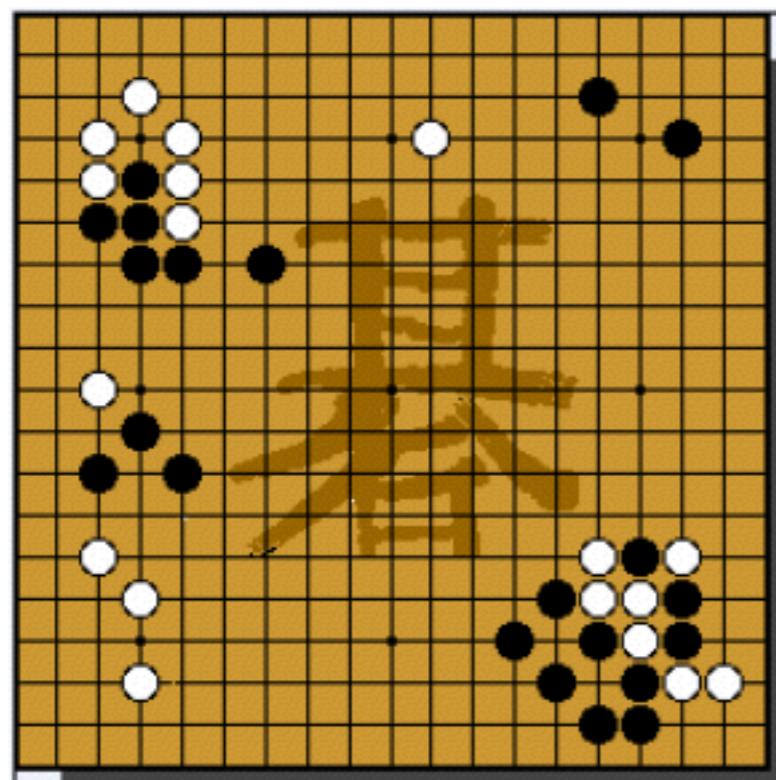


Figure 1 Go game

扩展：测量压力

UserID:

Color buttons

clear

A main login interface featuring a 9x9 grid. The grid has rows labeled 1 through 9 and columns labeled 1 through 9. There are several black squares representing 'star' points at (3,7), (5,5), (7,7), (3,3), and (7,3). Some cells are shaded gray. Buttons at the bottom include 'Login' and 'Don't show indicators'.

star

Shaded cell

1 2 3 4 5 6 7 8 9

9  
8  
7  
6  
5  
4  
3  
2  
1

1 2 3 4 5 6 7 8 9

Login      Don't show indicators

Figure 22 Main login interface

# Recognition-Based

# Deja Vu

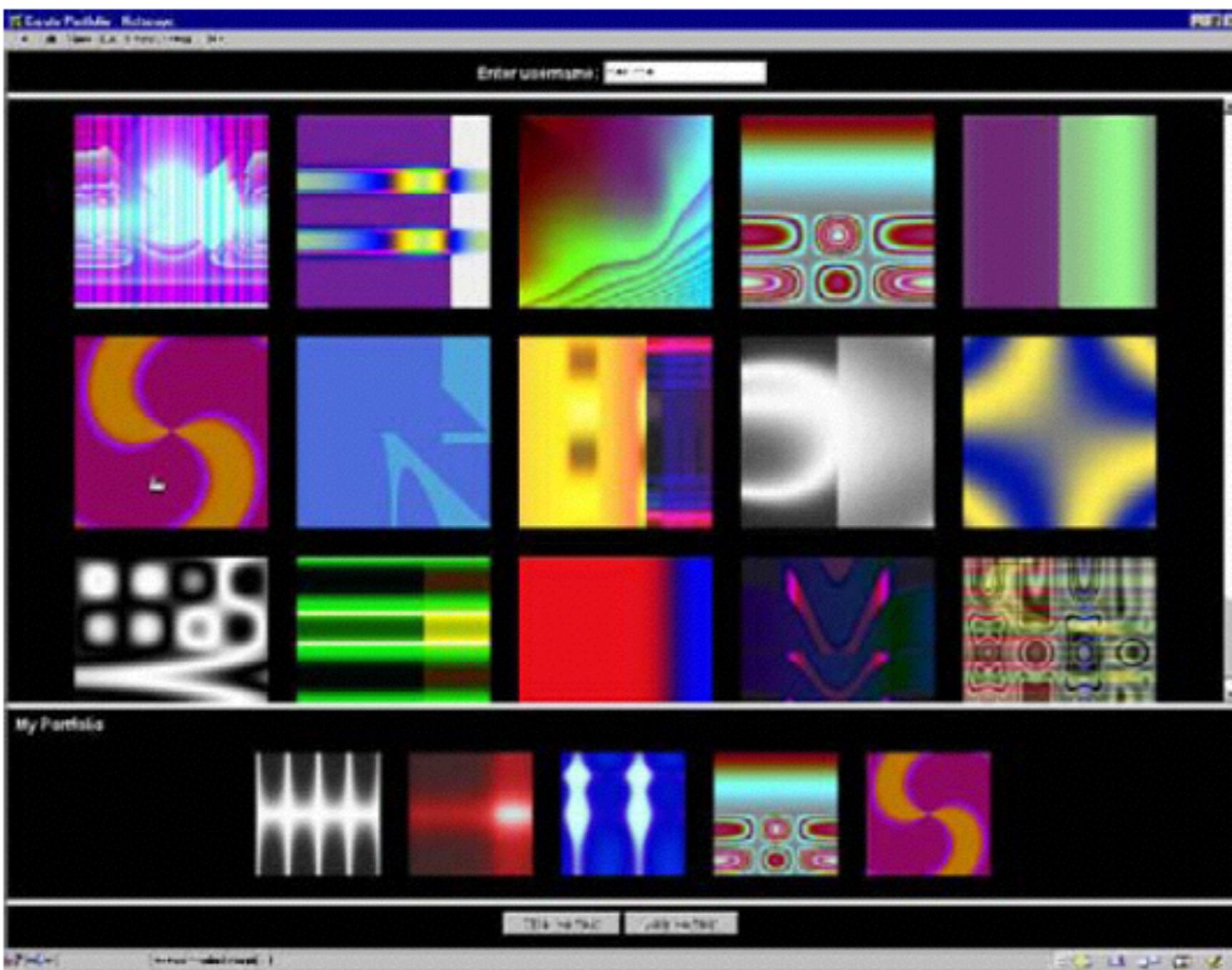


Figure 8 Déjà Vu [Dhamija and Perrig 2000]

## Recognition-Based

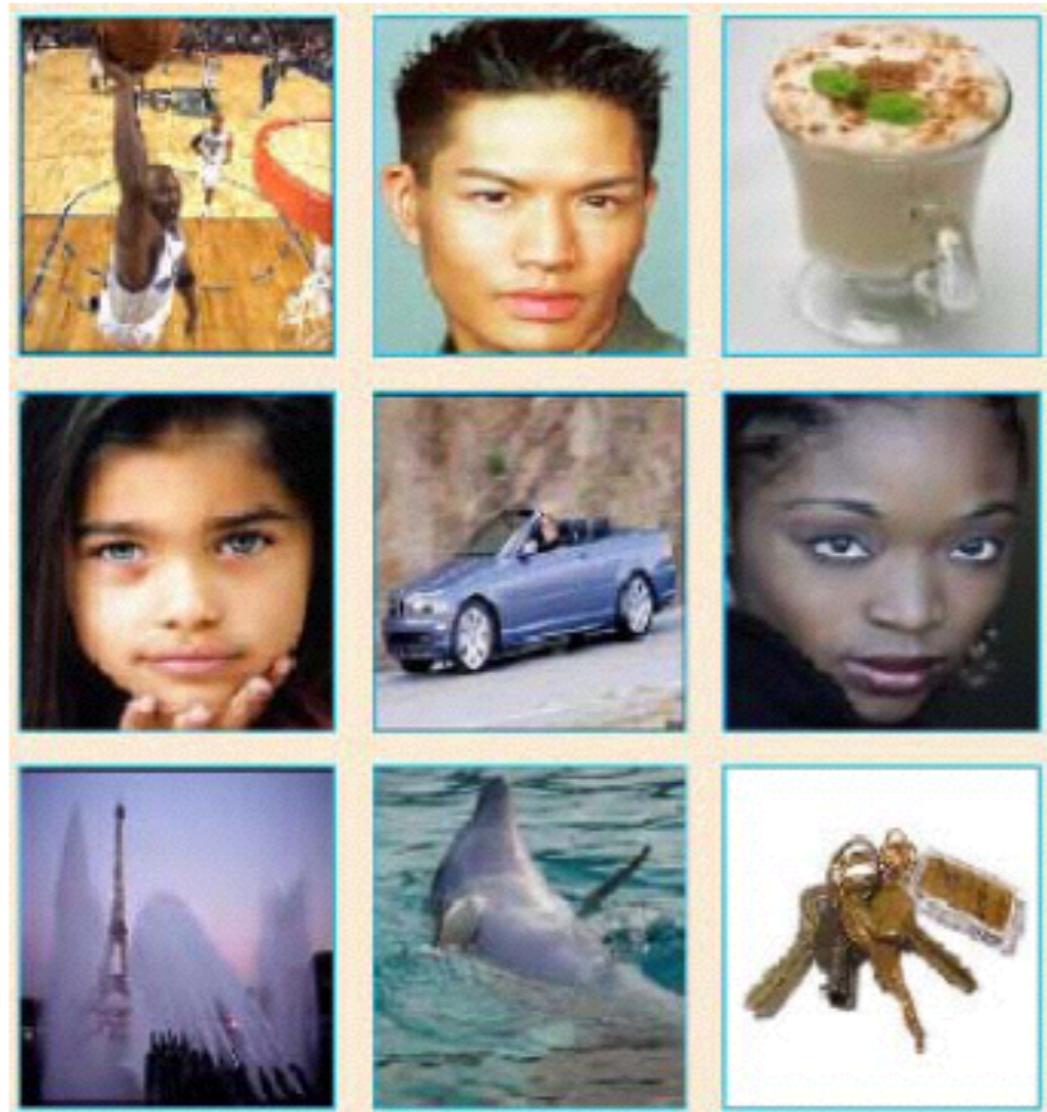
## PassFaces



Figure 6 Passfaces™ [Passfaces 2006]

- recognise images from decoy images
- face、random art、everyday objects、icons
- challenge-response
- system side security
- 图像来源：自己 vs 系统
- 注册时间：3-5分钟
- decoy的选择
- 口令空间

# Recognition-Based Story



- 图像之间有序
- 口令空间更大
- 记忆有负担

Figure 7 Story scheme [Davis et al. 2004]

# Recognition-Based

# Use your Illusion

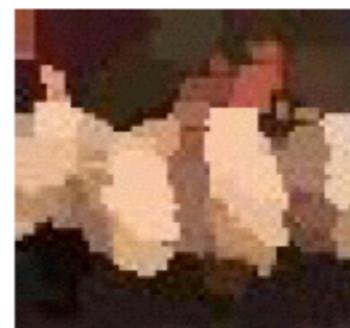
可用性干扰



马赛克去除技术

Please memorize  
the three distorted  
images shown above.

OK



# Cued Recall-Based

# Passpoints

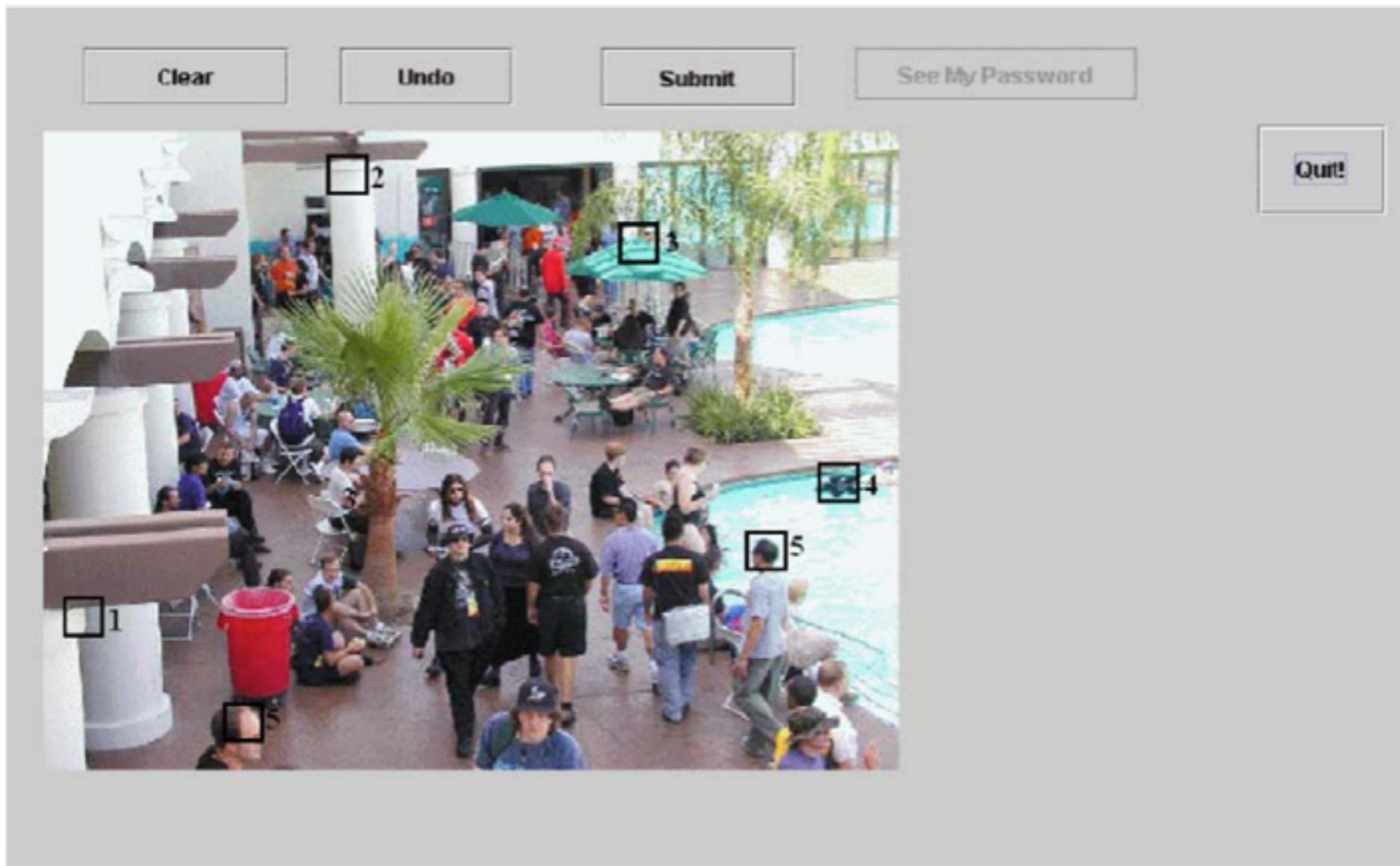


Figure 3 VisKey [Sfr 2006]

Fig. 2. Example of participant password with tolerance and click order displayed.

- 图像中的位置是秘密
- 点击输入
- 需要工具来注册
- 注册: 171秒
- login: 19秒
- 14\*14像素容忍度

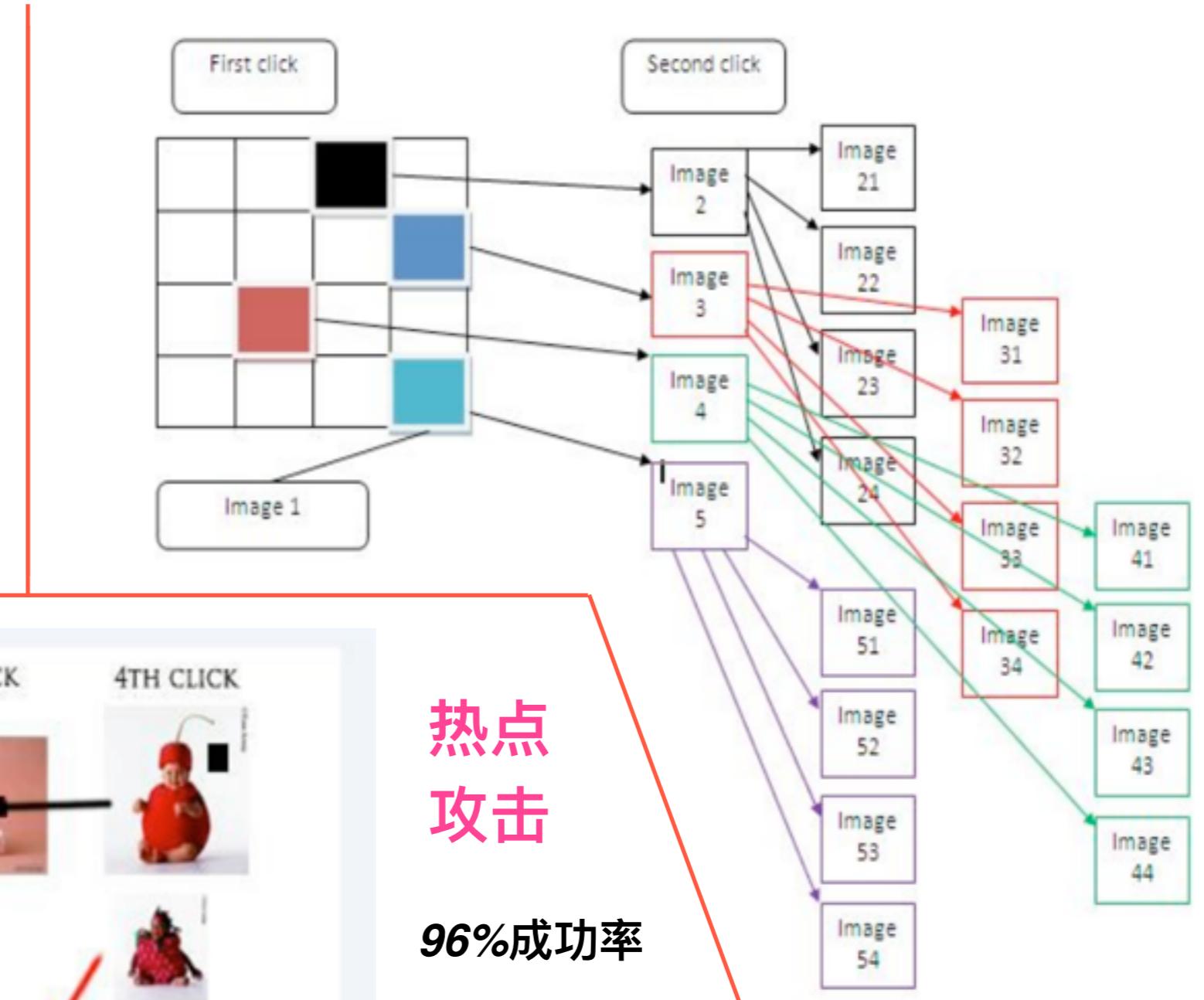
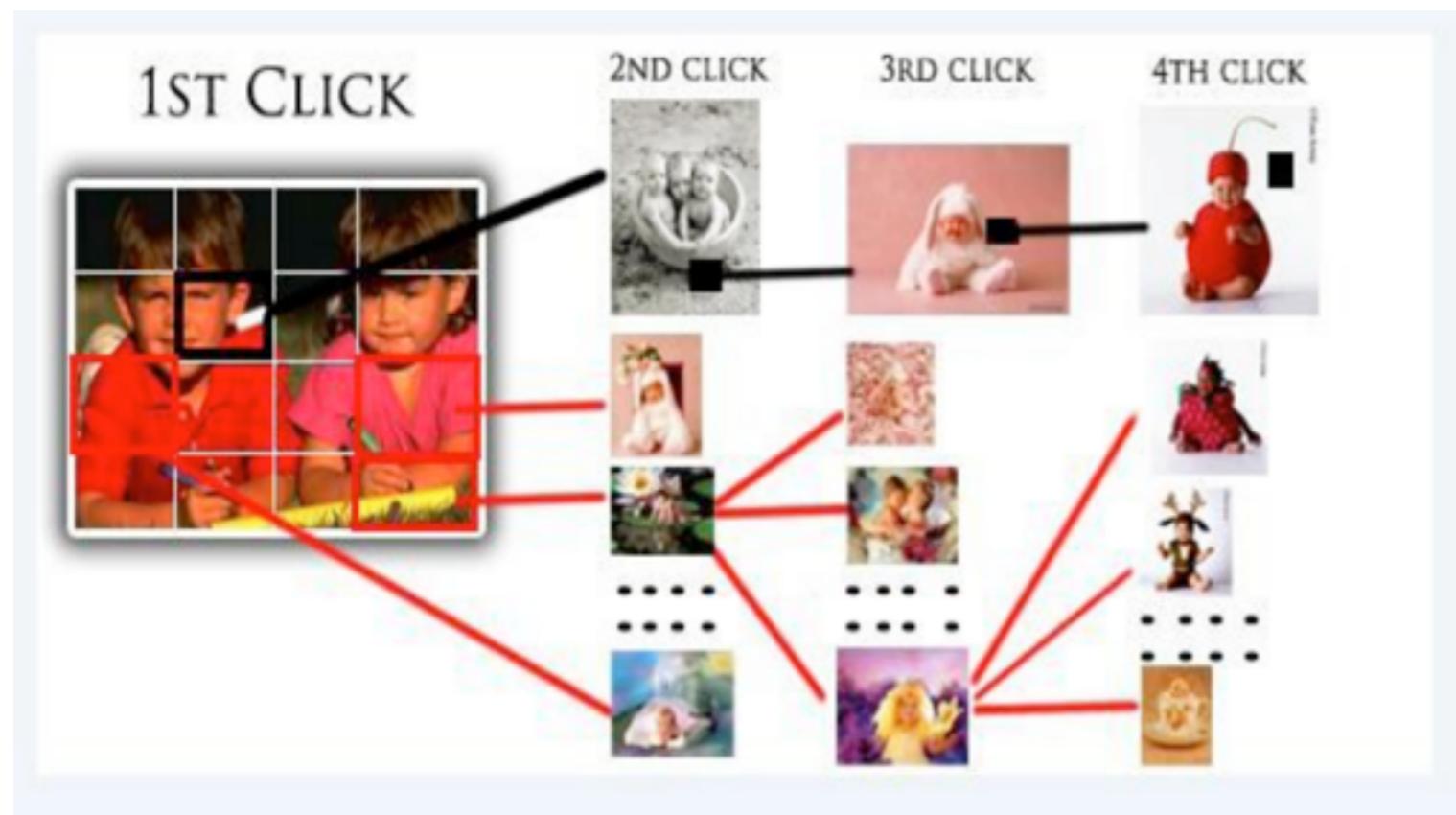
热点攻击

多个口令

一对多

# CCP: Cued Click Points

- 一对一线索
- implicit feedback
- 避免简单模式



- 注册: 25秒
- Login: 7秒



- **viewport**
- 随机化
- 避免hotspots
- 创建: 50秒
- Login: 8秒



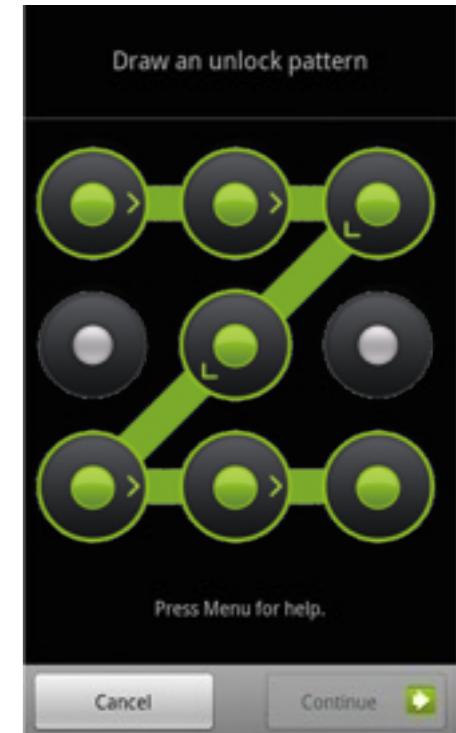
# My App is My Password!

# Background

- *Graphical password*

- \* more applicable on smartphone than text password
- \* vulnerable to shoulder surfing attack

- \* **existing graphical password require user proactively memorise password**

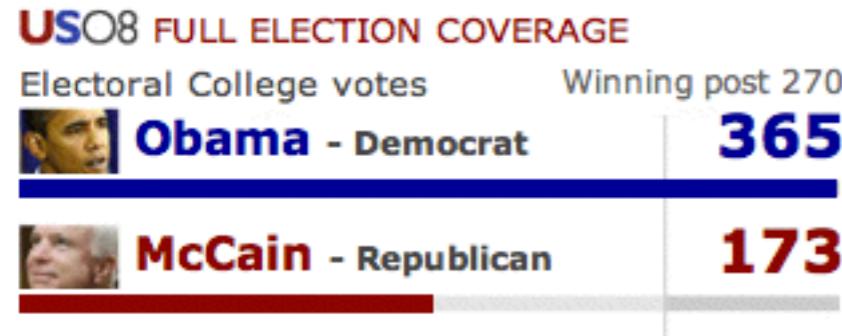


**Graphical  
password  
based  
existing  
memory**

- Authentication based existing memory

- \* weak password
- \* security questions
- \* dynamic security questions
- \* autobiographical authentication

# Password Alternatives



2008.09.17

## 后备认证

<http://news.bbc.co.uk/2/hi/7622726.stm>

### Hackers infiltrate Palin's e-mail

**Hackers have broken in to the e-mail of the US Republican vice-presidential candidate, Alaska Governor Sarah Palin.**

The hackers, who targeted a personal Yahoo account, posted several messages and family photos from her inbox.

The campaign of running mate John McCain condemned their action as "a shocking invasion of the governor's privacy and a violation of the law".

The hacking comes amid questions about whether Mrs Palin used personal e-mail to conduct state business.

According to law, all e-mails relating to the official business of government must be archived and not destroyed. However, personal e-mails can be deleted.

Mrs Palin is currently under investigation in Alaska for alleged abuse of power while governor.



Sarah Palin has been campaigning for Republican running mate John McCain

[gov.palin@yahoo.com](mailto:gov.palin@yahoo.com)

Where did you meet your spouse?

Wasilla High School

[http://wikileaks.org/wiki/VP\\_contender\\_Sarah\\_Palin\\_hacked](http://wikileaks.org/wiki/VP_contender_Sarah_Palin_hacked)

2008

# Exploring Capturable Everyday Memory for Autobiographical Authentication

**Sauvik Das**

Carnegie Mellon University

sauvik@cmu.edu

**Eiji Hayashi**

Carnegie Mellon University

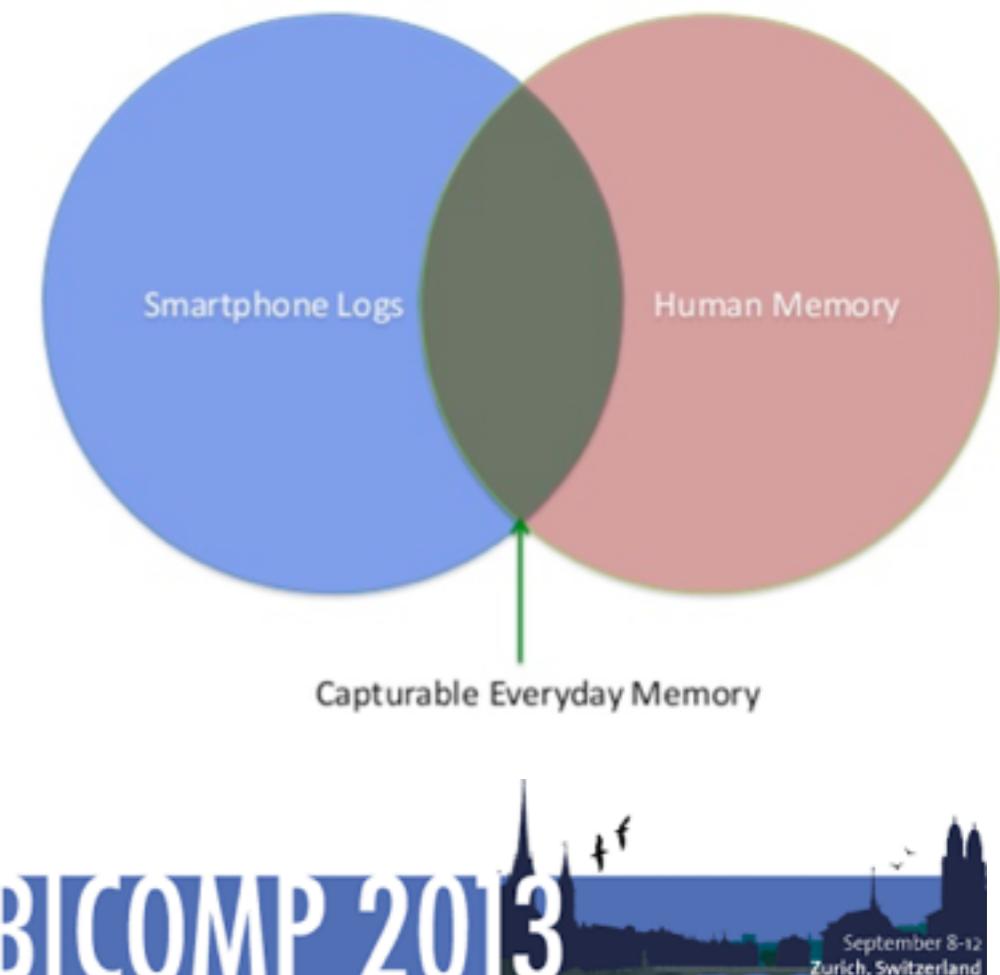
ehayashi@cs.cmu.edu

**Jason Hong**

Carnegie Mellon University

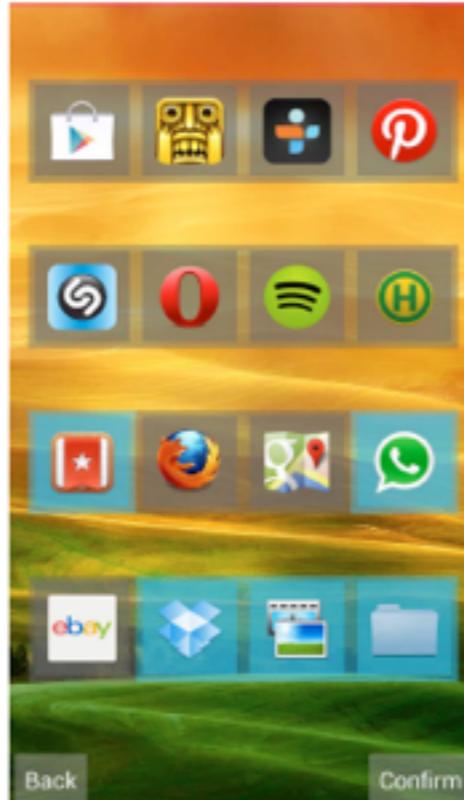
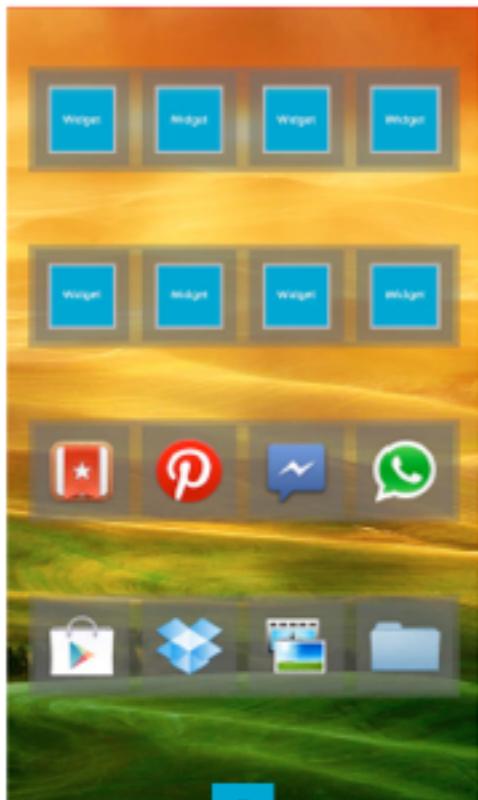
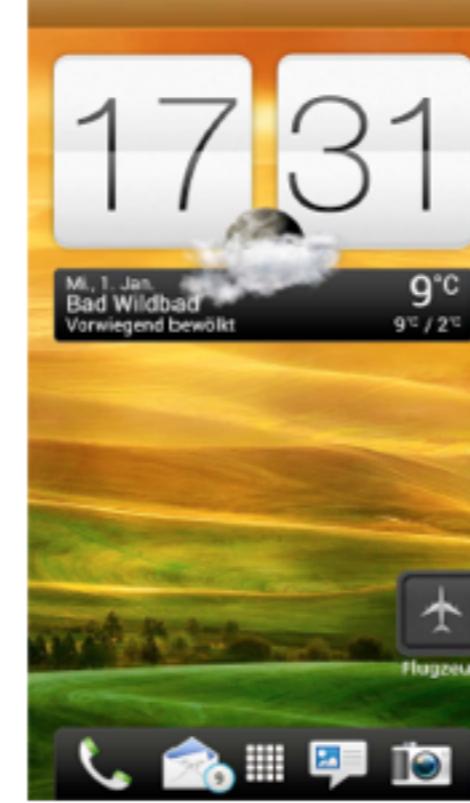
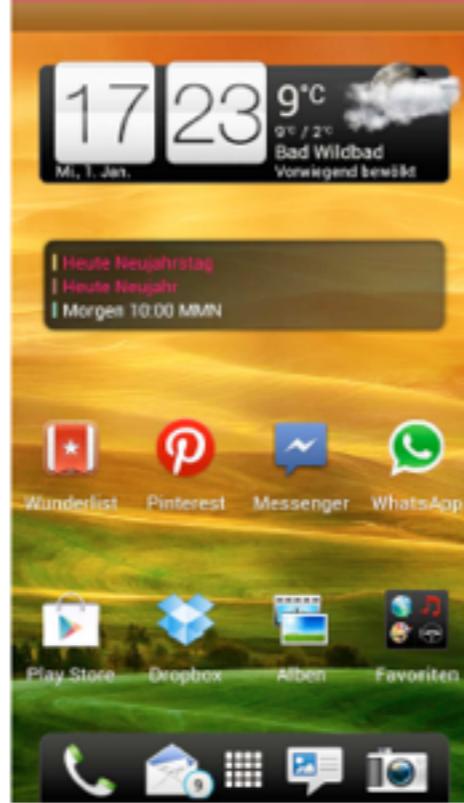
jasonh@cs.cmu.edu

QType	Likert-scale prompts in Study 2.
FBApP	What application did you use on <time>?
FBLoc	Where were you on <time>?
FBOCall	Who did you call on <time>?
FBInCall	Who called you on <time>?
FBOSMS	Who did you SMS message on <time>?
FBInSMS	Who SMS messaged you on <time>?
FBIntSrc	What did you search the internet for on <time>?
FBIntVis	What website did you visit on <time>?
NAOSMS	Name someone you SMS messaged in the last 24 hours.
NAInSMS	Name someone who SMS messaged you in the last 24
NAOCall	Name someone you called in the last 24 hours.
NAInCall	Name someone who called you in the last 24 hours.
NAApp	Name an application you used in the past 24 hours.



# Password Alternatives

## APP图标布局认证



***Using Icon  
Arrangement for  
Fallback  
Authentication  
on Smartphones***

***Poster  
@ CHI 2014***

# Password Alternatives

## 动态安全问题

Backup Authentication

Who did you call yesterday?

Please choose one of the following answers:

Andy

Samantha

None of them

Antonio

3 of 21

Backup Authentication

Which photo did you take last week?

Please choose one of the following photos:



None of them

3 of 21

Category	Question + Timespan
SMS (out)	Who did you text [Y   LW]?
SMS (in)	Who texted you [Y   LW]?
Call (out)	Who did you call [Y   LW]?
Call (in)	Who called you [Y   LW]?
App	Which App did you use [Y   LW]?
App Install	Which app did you install/update [Y   LW]?
Photos	Which photo did you take [Y   LW]?

Y=Yesterday; LW=Last Week

***I Know What You  
Did Last Week!  
Do You? Dynamic  
Security  
Questions for  
Fallback  
Authentication  
on Smartphones***

**@ CHI 2015**

# Password Alternatives

## 动态安全问题 - APP安装

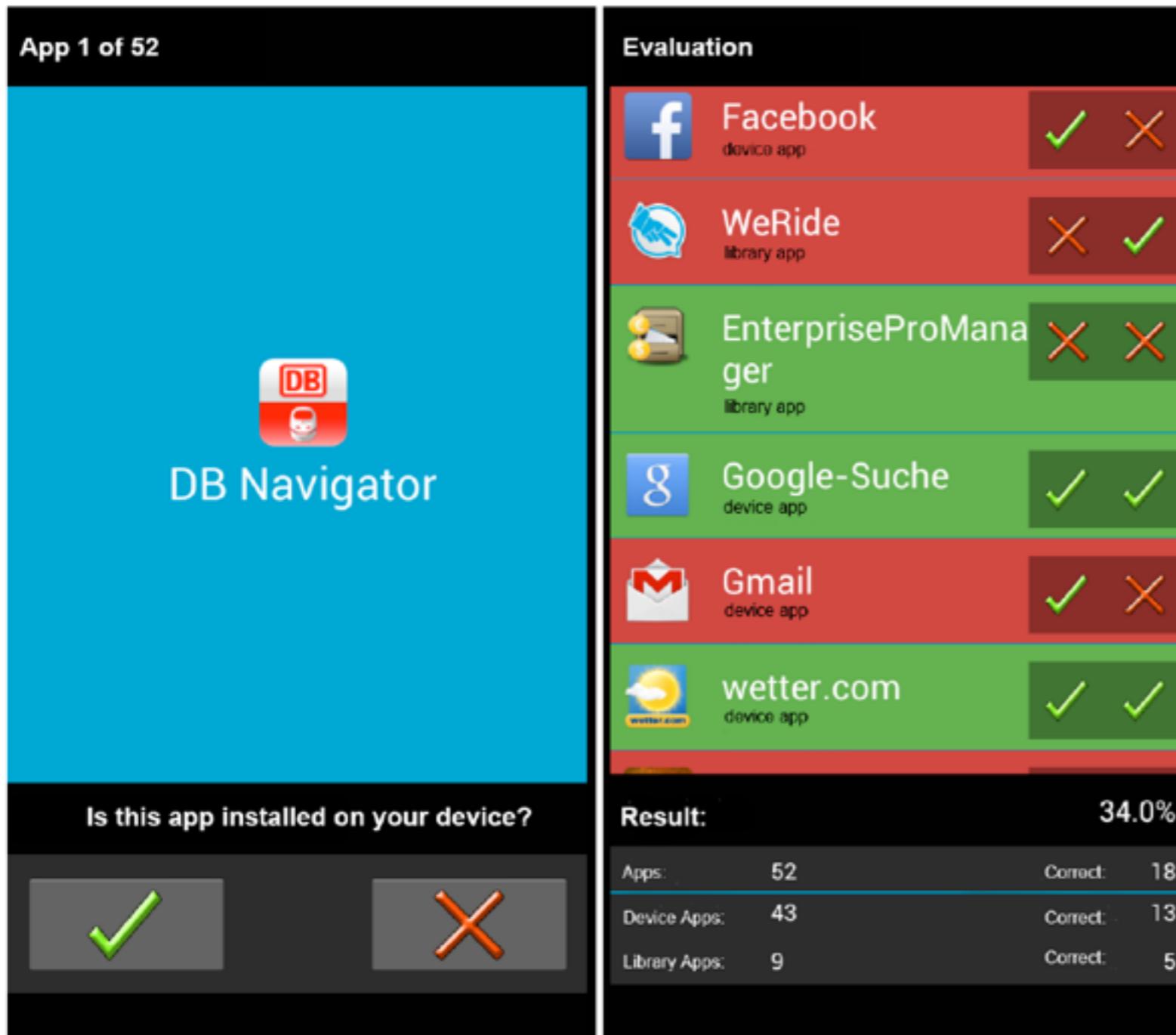


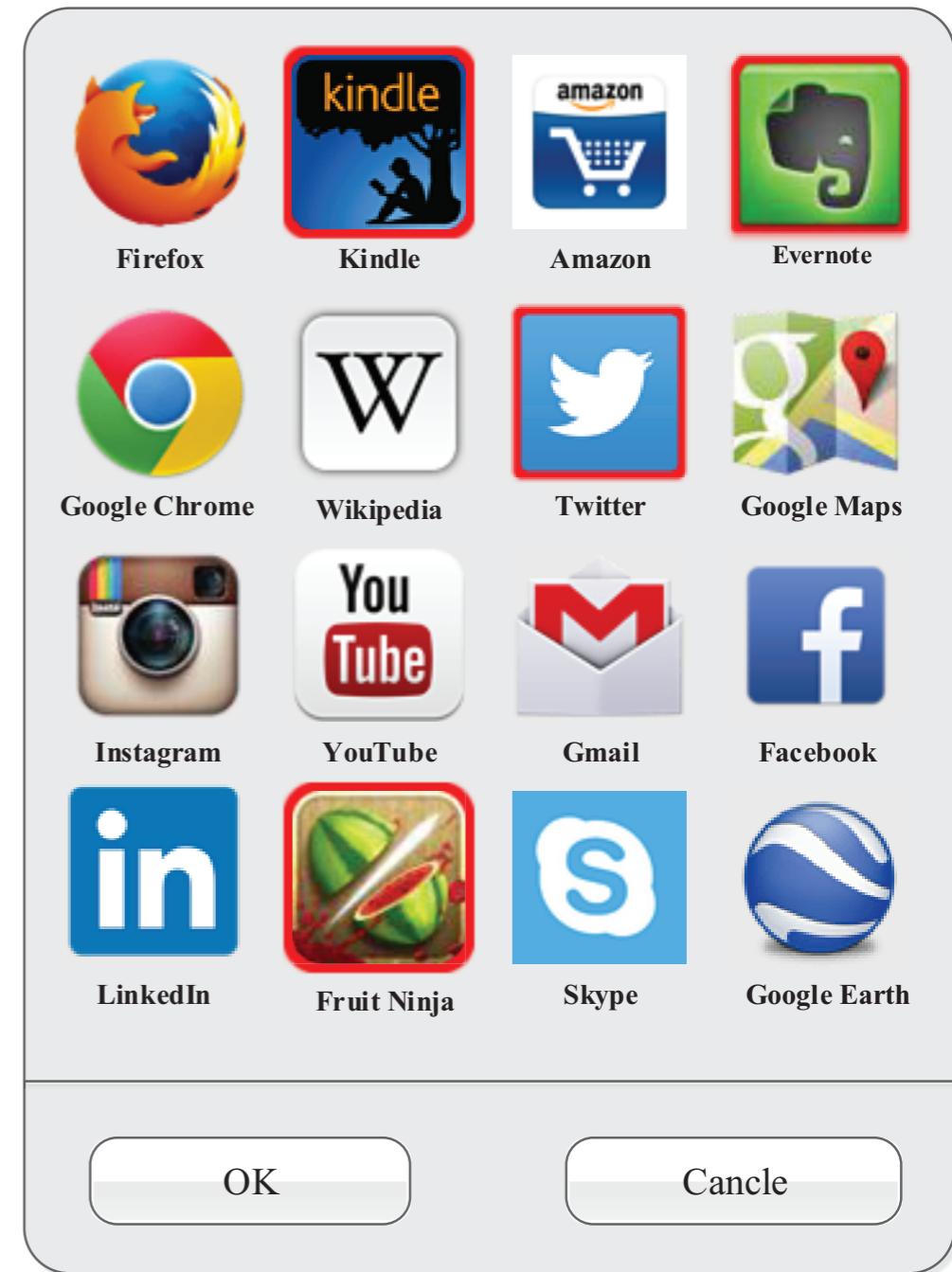
Figure 1. Screenshots of the study application. The left one shows an exemplary question that users were quizzed during the study. The right one is an overview of the performance of a participant during the study. Original language: German.

***Locked Your  
Phone? Buy a  
New One? From  
Tales of Fallback  
Authentication on  
Smartphones to  
Actual Concepts***

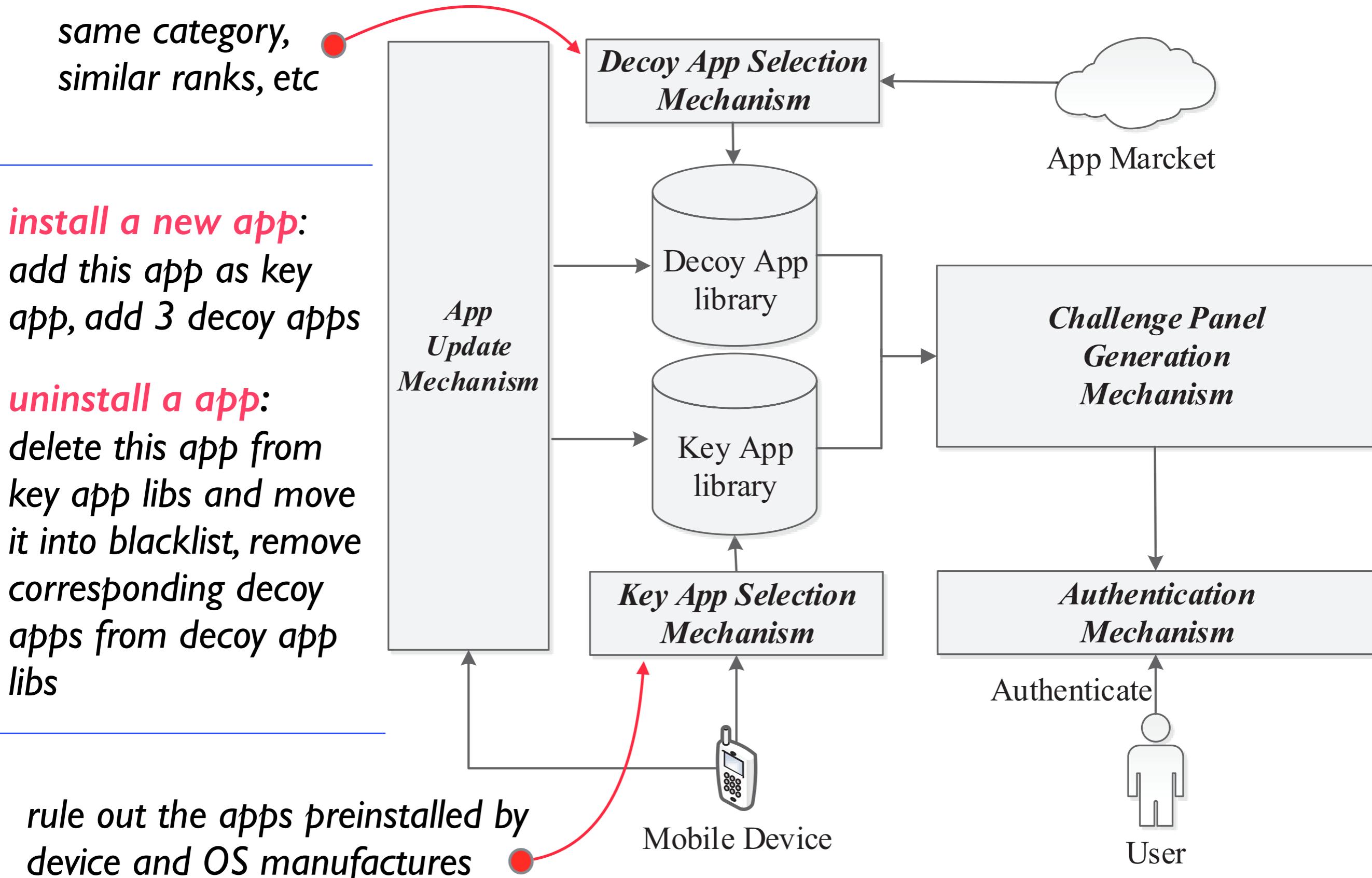
***@ MobileHCI  
2015***

# PassApp Concept

**PassApp**  
*is a novel recognition-based  
graphical password which  
utilises user's  
installed apps  
on their mobile devices  
as password*



# PassApp Mechanism

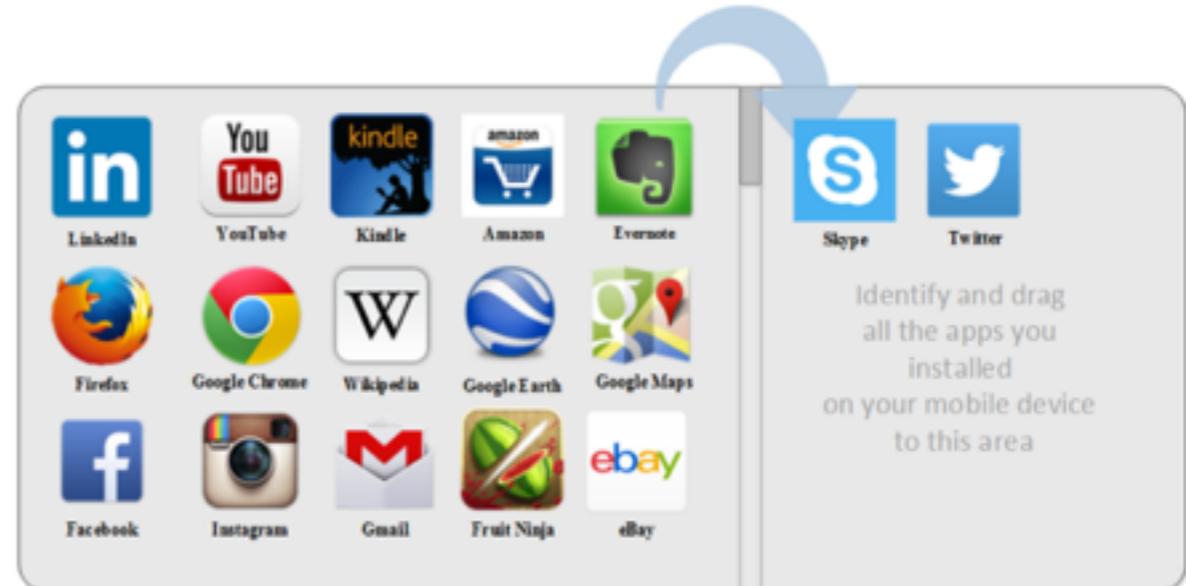




# User Study

Day 1

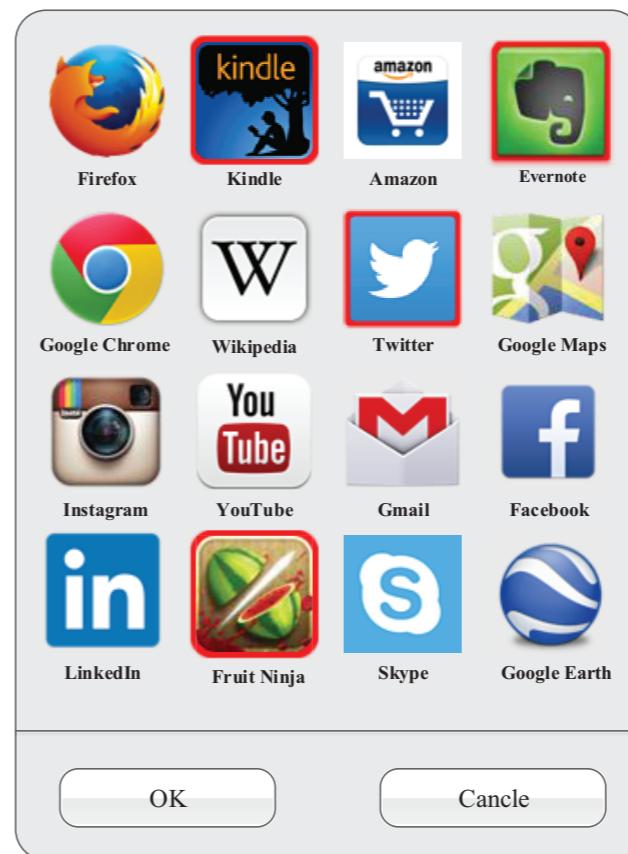
*User Study 1:  
How well can users  
correctly recognise the apps  
they have installed?*



42 participants

Day 2

*User Study 2:  
How well can PassApp  
perform on usability and  
user experience?*



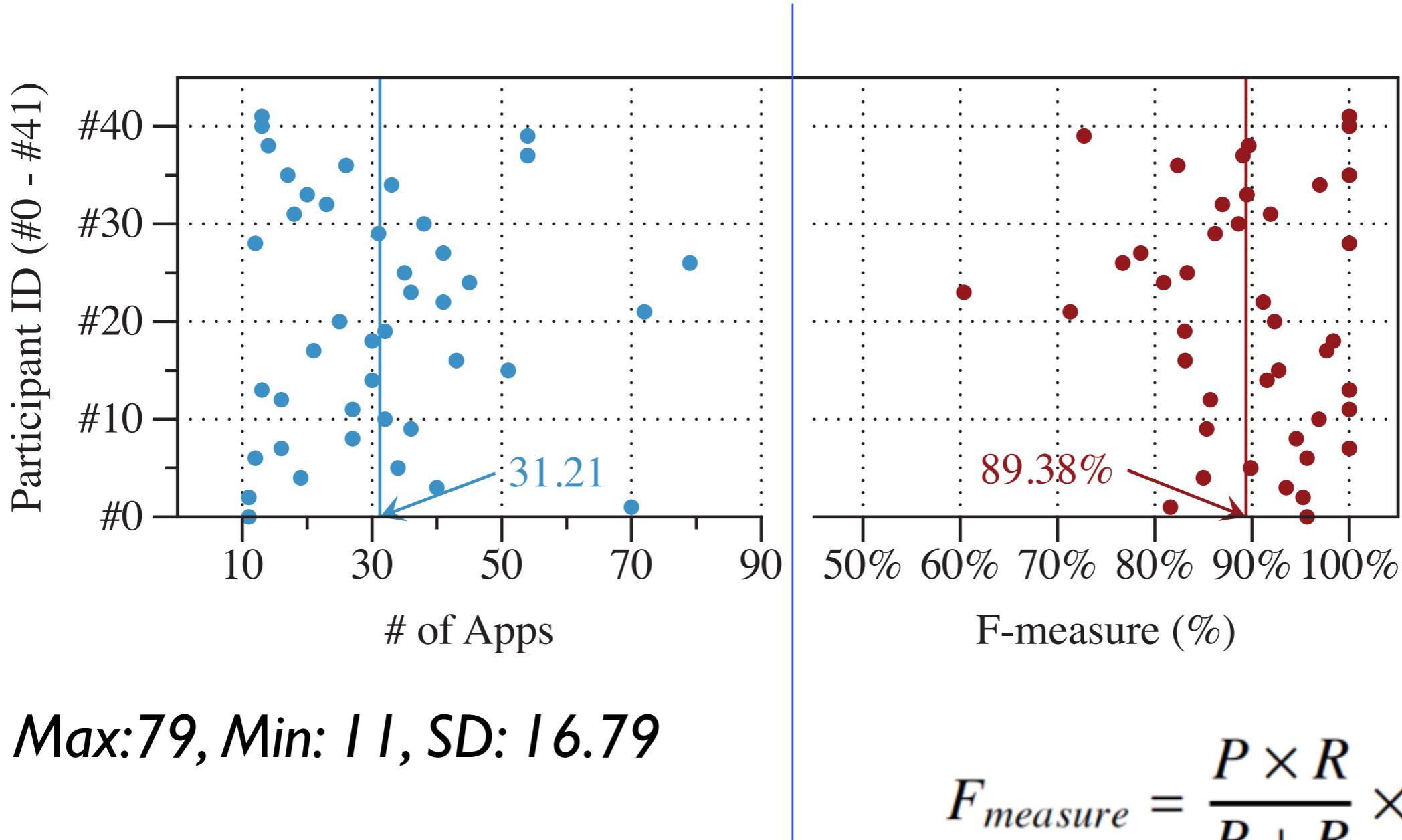
unlock 10 times

42 \* 10

Login Time

Success Rate

# Memory about Installed Apps



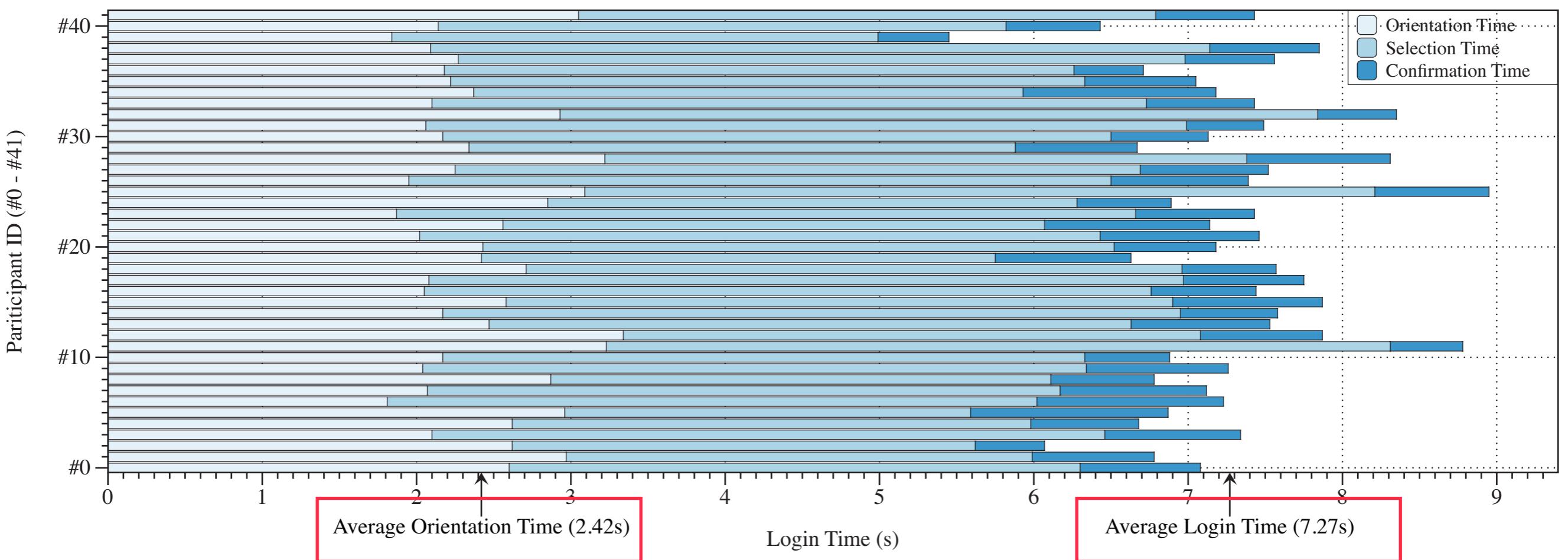
$$F_{measure} = \frac{P \times R}{P + R} \times 2$$

$$P(precision) = \frac{\sum \text{picked installed apps}}{\sum \text{all apps picked}}$$

$$R(recall) = \frac{\sum \text{picked installed apps}}{\sum \text{all installed apps}}$$

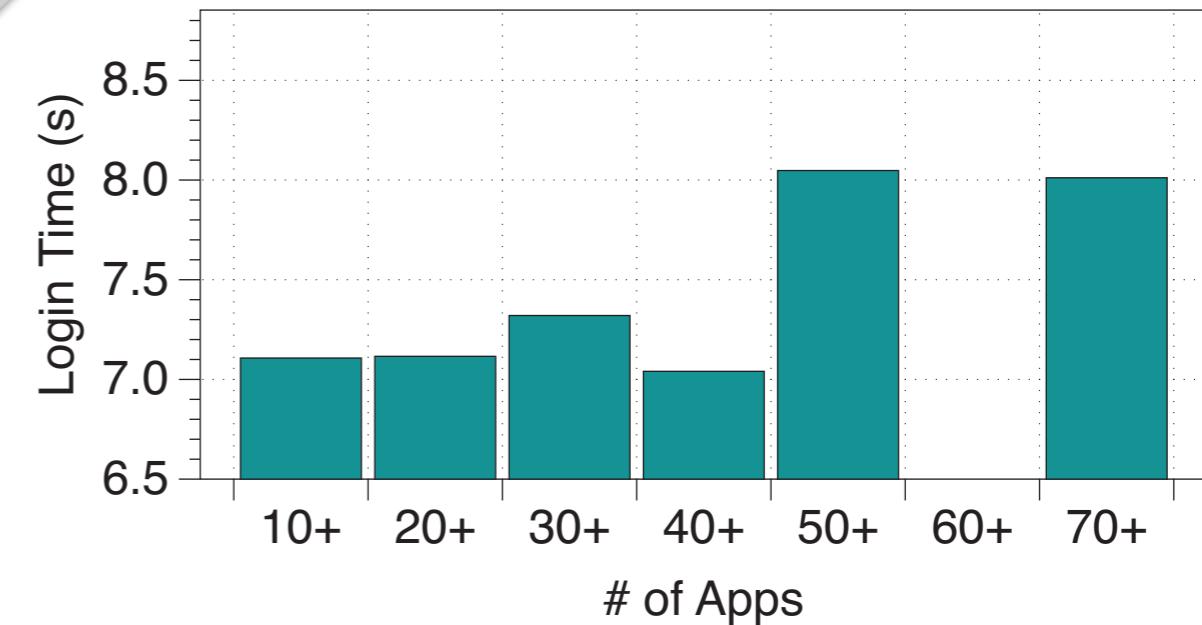
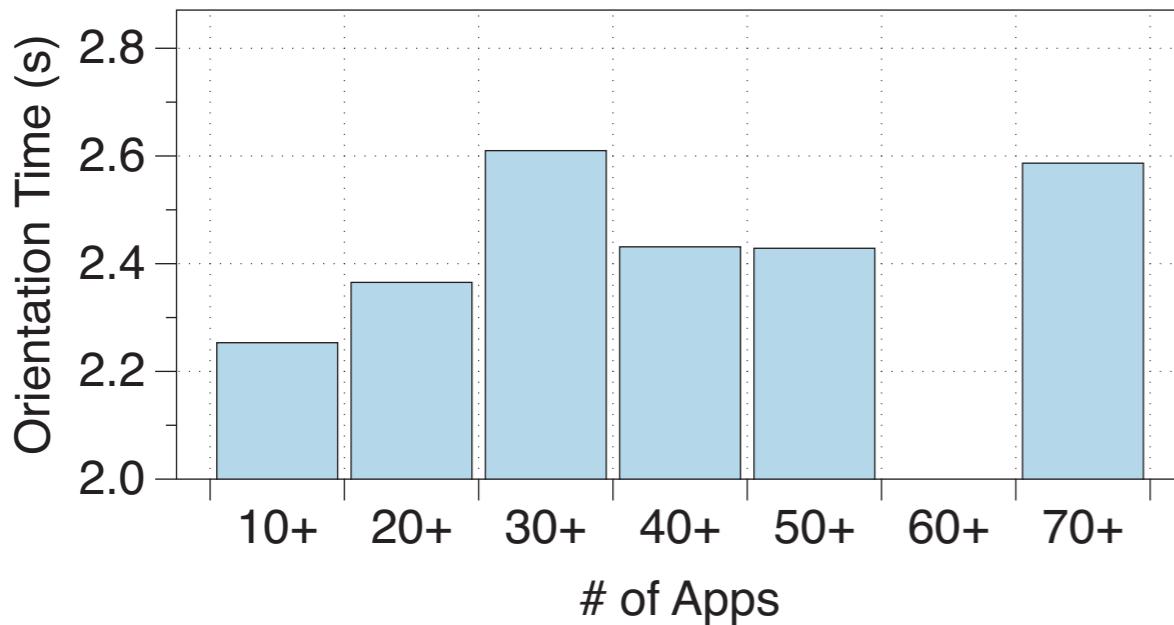
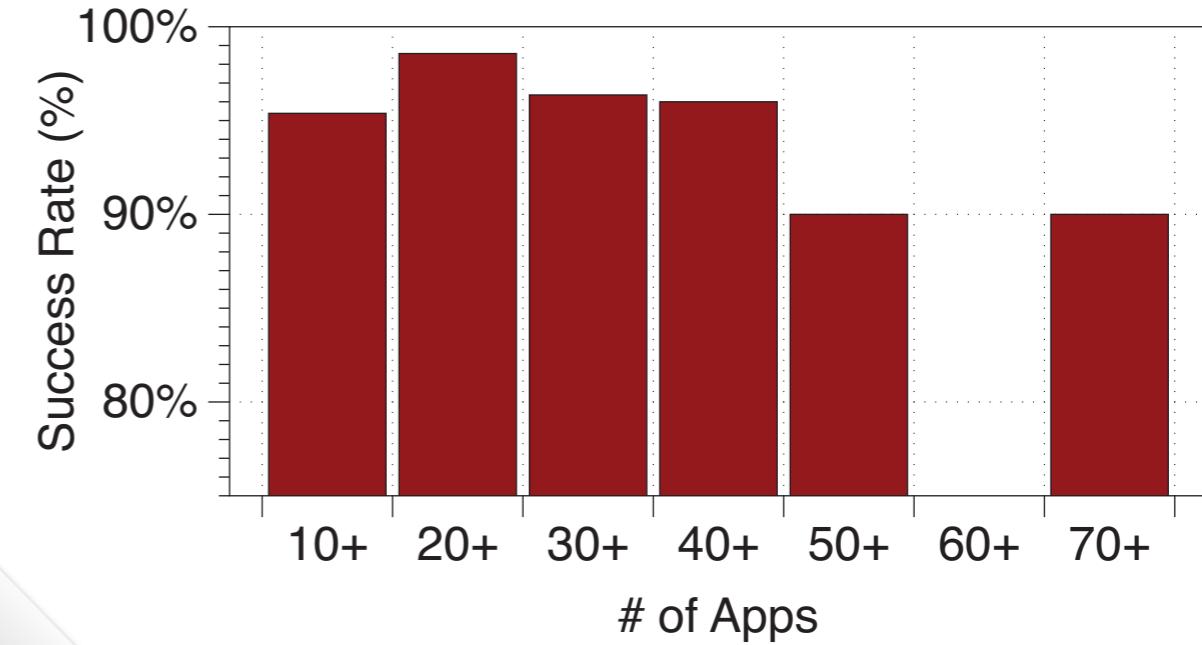
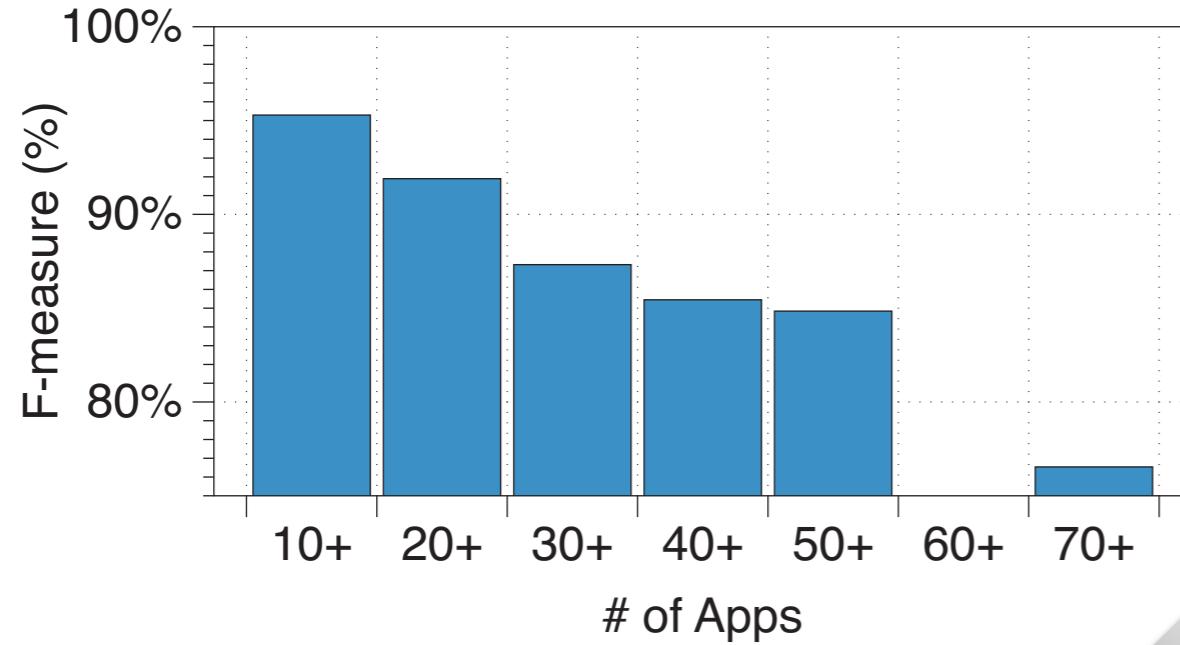
# Login Time and Success Rate

Scheme	<b>PassApp</b>	Cognitive Auth [35]	Convex Hull Click [37]	Déjà vu [14]	Passfaces [10]	UYI [23]
Login Time	<b>7s (5s-10s)</b>	90-180s	72s	32-36s	14-88s	12-26s
Success Rate	<b>&gt;95%</b>	>95%	90%	90-100%	72-100%	89-100%

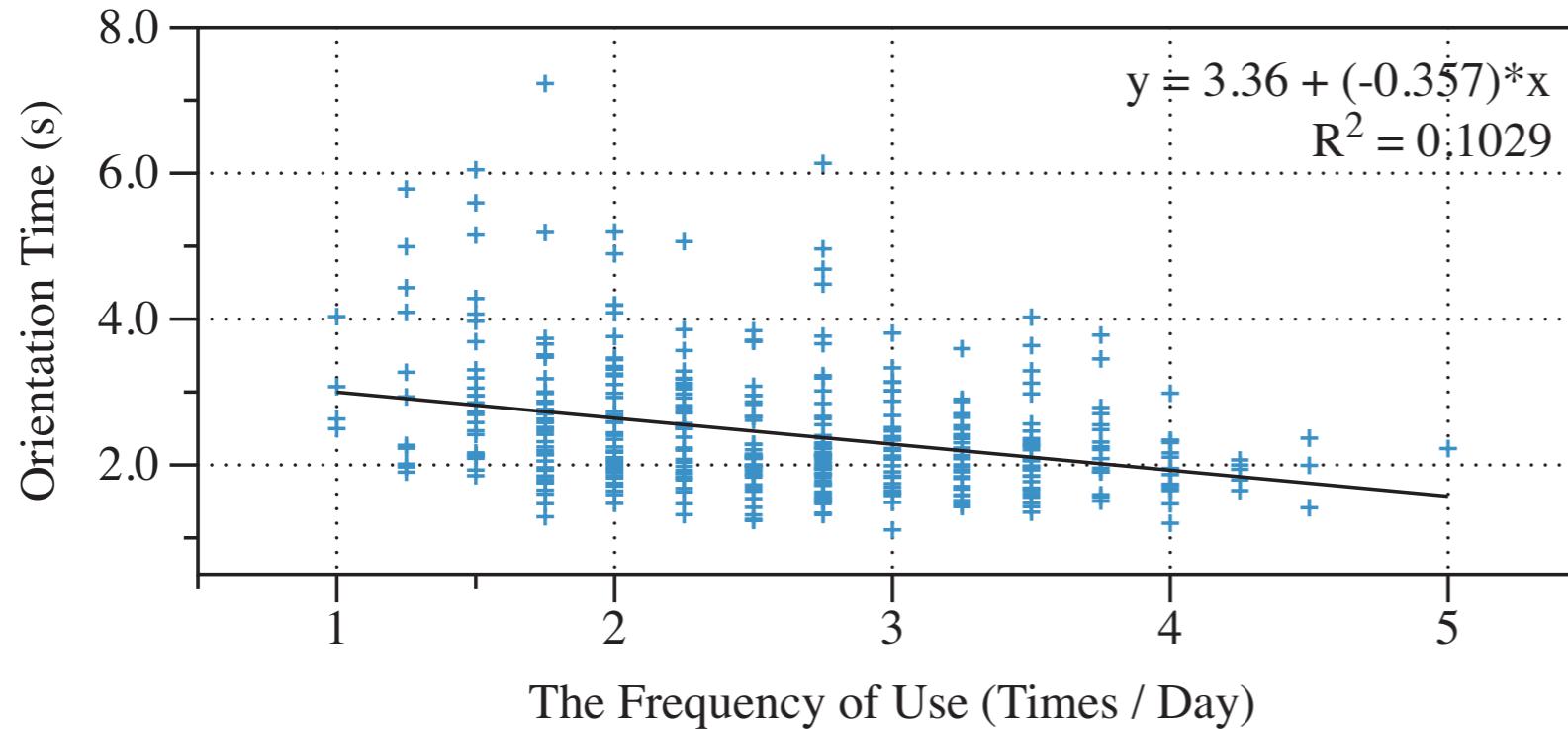


Average confirmation time: 0.76s

# *Number of Key Apps & Usability Indices*

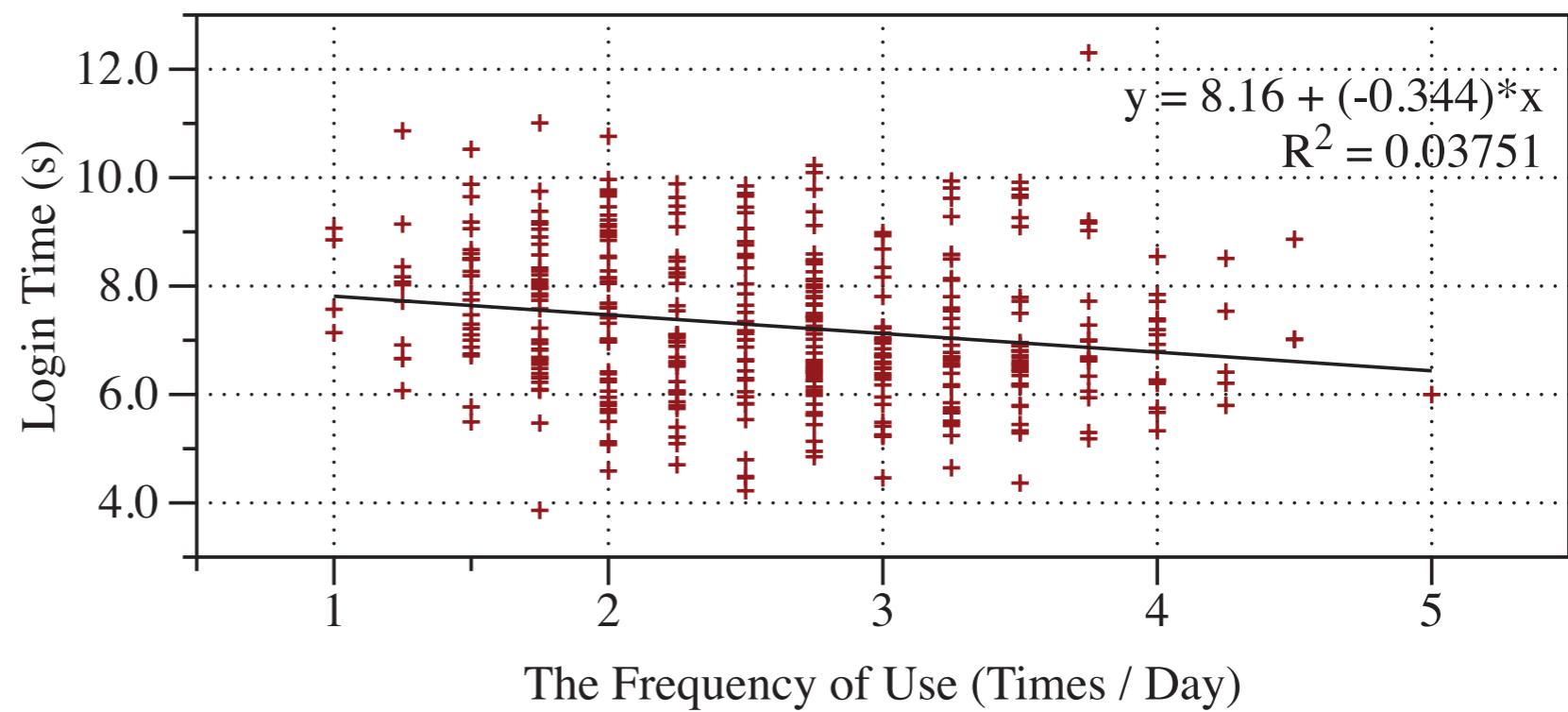


# *Frequency of Using Apps & Usability Indices*



28.38% <0.2 times/days  
21.66% 0.2 -0.5 t/d  
23.11% 1-2 t/d  
12.36% 3-5 t/d  
14.49% >5 t/d

*In user study 1,  
Participant need  
complete a web  
survey to  
mark the frequency of  
using the installed  
apps*



# Security Analysis

## Brutal-force Attacks

$$1/\binom{16}{4} = 1/1820.$$

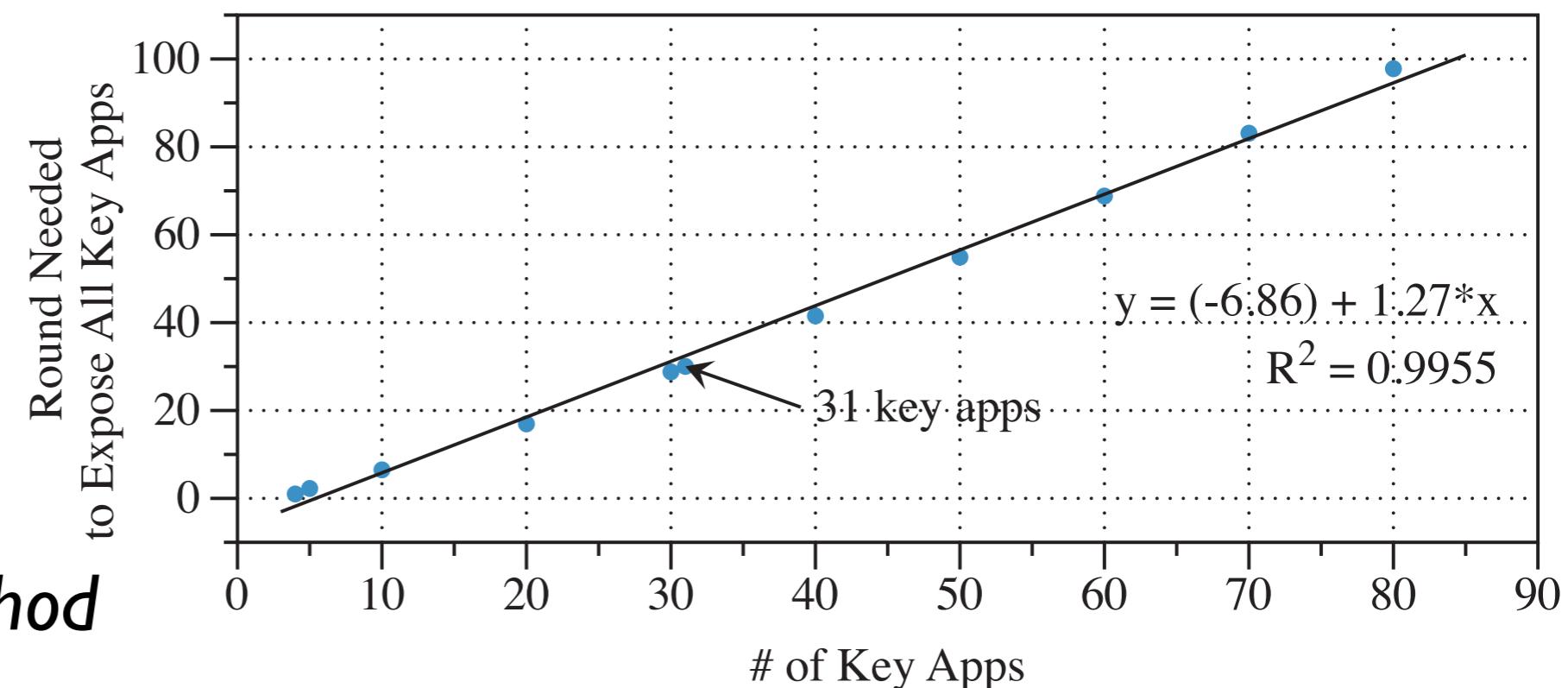
0.055%

## One-time shoulder Surfing Attacks

$$E = \sum_{i=0}^4 \left( \frac{\binom{4}{i} \times \binom{s-4}{4-i}}{\binom{s}{4}} \times i \right)$$

## Multi-time shoulder Surfing Attacks

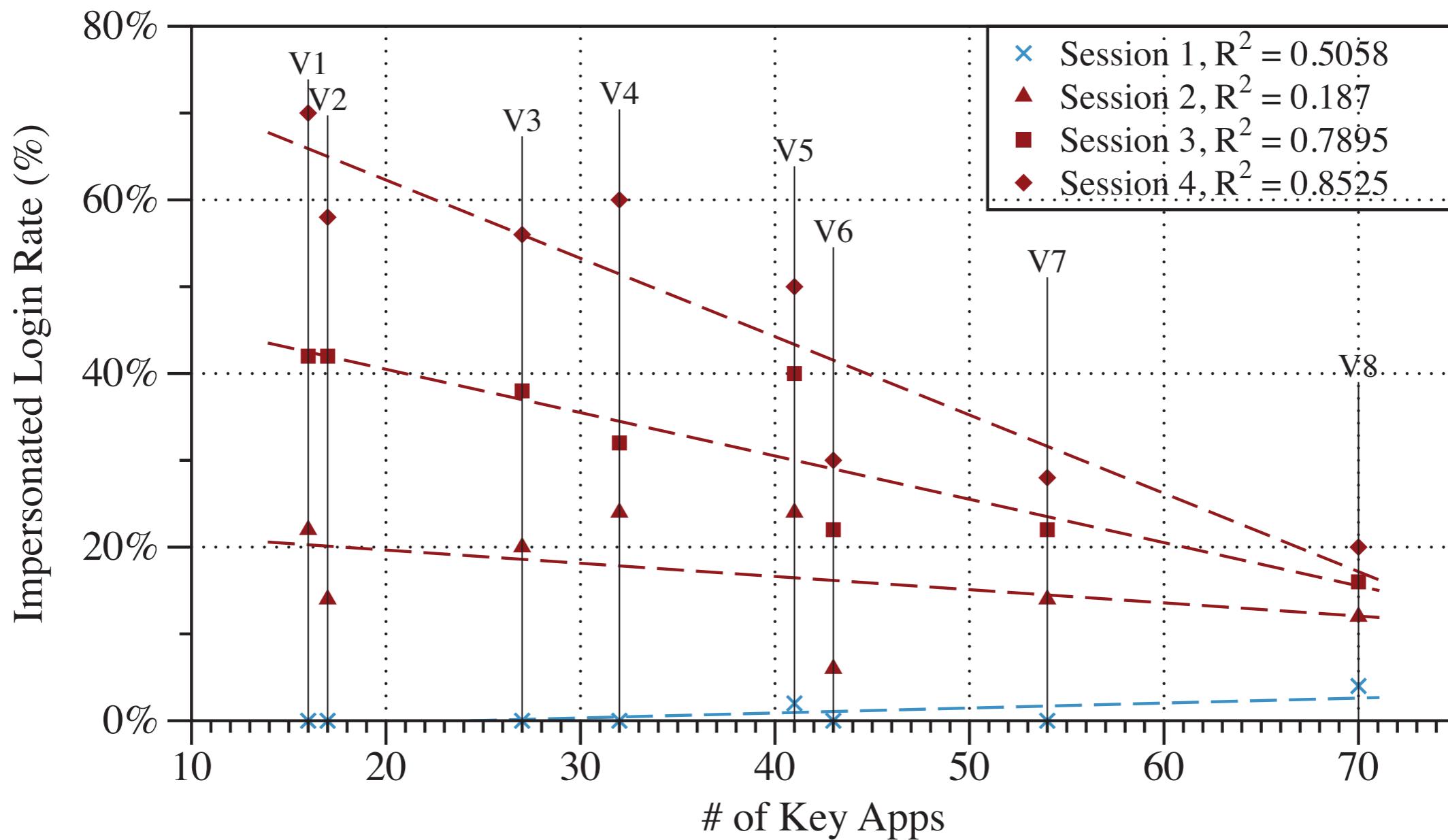
Monte Carlo Method



## Session 1: Guessing Attacks

## Session 2-4: Acquaintance Attacks

Session	1	2	3	4
Successful Logins	3	68	127	186
Percentage	0.75%	17.00%	31.75%	46.50%



# Discussion

---

- Key app selection
  - \* too short or too many, popular apps, communication apps
- Decoy app selection
  - \* app market, device manufacture, OS, language, etc
- Challenge panel generation ( $n$  key \*  $m$  decoy \*  $r$  rounds)
- Login time (challenge, backup authentication)
- Participant (field study in the future)
- Daily memory about other graphical elements
  - photography, wallpapers, screenshots, avatars, etc
  - privacy vs security vs usability

# Conclusion

---

- *PassApp is the first graphical password that utilizes user's existing memory about installed apps as password*
  - \* *without registration stage*
  - \* *without memory burden*
- *PassApp perform better usability than most graphical password*
  - \* *acceptable login time: 7.27s (6.51s)*
  - \* *high success rate: >95%*
- *PassApp has sufficient security than most graphical password*
  - \* *brute-force attacks (0.055%) and dictionary attacks (0.75%)*
  - \* *shoulder surfing attacks: average 30 times*
  - \* *acquaintance attacks: can to some extent withstand (challenge)*

# 如何评价图形口令的 可用性和安全性

## 用户 & 环境

- 专家
- 频繁使用用户
- 不频繁使用用户
- 特殊群体

- 使用设备
  - 手机、PAD、PC
  - 网络、屏幕、
- 使用环境
  - 高风险
  - 低风险

- 口令初始化
  - 用户自己产生 vs 系统自动产生
  - 口令可预测 vs 训练时间 vs 口令重用
- Login
  - 成功率、错误率
  - 记忆测量、记忆干扰
- 口令改变和重置
  - 不容易通信、临时的非图形口令

- 猜测攻击

- 在线：延迟、次数、锁定
- 离线：hash、salting、
- 图形口令：checker
- 暴力攻击：彩虹表
- 字典攻击：face、hotspot

- 俘获攻击

- 肩窥攻击
- 交叉攻击
- 污渍攻击
- 个性化攻击

## 评估方法

- 专家评估 vs 用户实验 vs 实际使用
- 使用文本口令作为参照
- lab study vs field study
- 问卷、访谈
- 实验人数
- 多个session
- 基于Web：Amazon Mechanical Turk
- IRB：伦理审查
- 盲试

- 要求阅读如下论文：

→ *Florian Schaub et al. Exploring the Design Space of Graphical Passwords on Smartphones. In Proc. SOUPS'2013.*

下次上课测试！

- 课程项目组队和选题

下次上课是10月11日！

→ 10月10日前。

谢谢！

孙惠平

[sunhp@ss.pku.edu.cn](mailto:sunhp@ss.pku.edu.cn)