Information Security Engineering

2018.10.29

图形口令

北京大學 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

Human Computation回顾

1 概念

- 计算历史
- 定义
- 相关概念
- 人工智能

2 算法

- 算法描述
- 算法组成
- 算法正确性
- 参与动机

3 例子

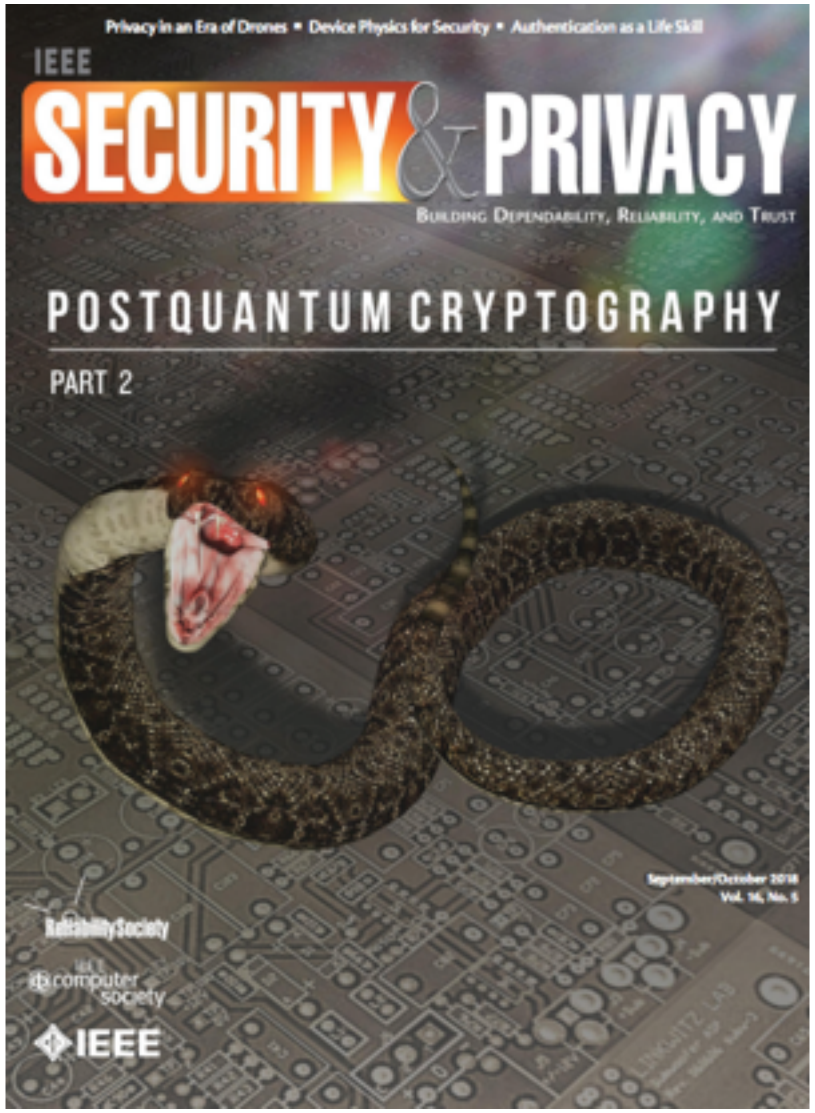
- ESP
- Citizen科学
- Amazon Turk
- 众包

4 CAPTCHA

- 定义和历史
- 文本类型
- 技术和攻击
- 其余类型

Reading Paper回顾

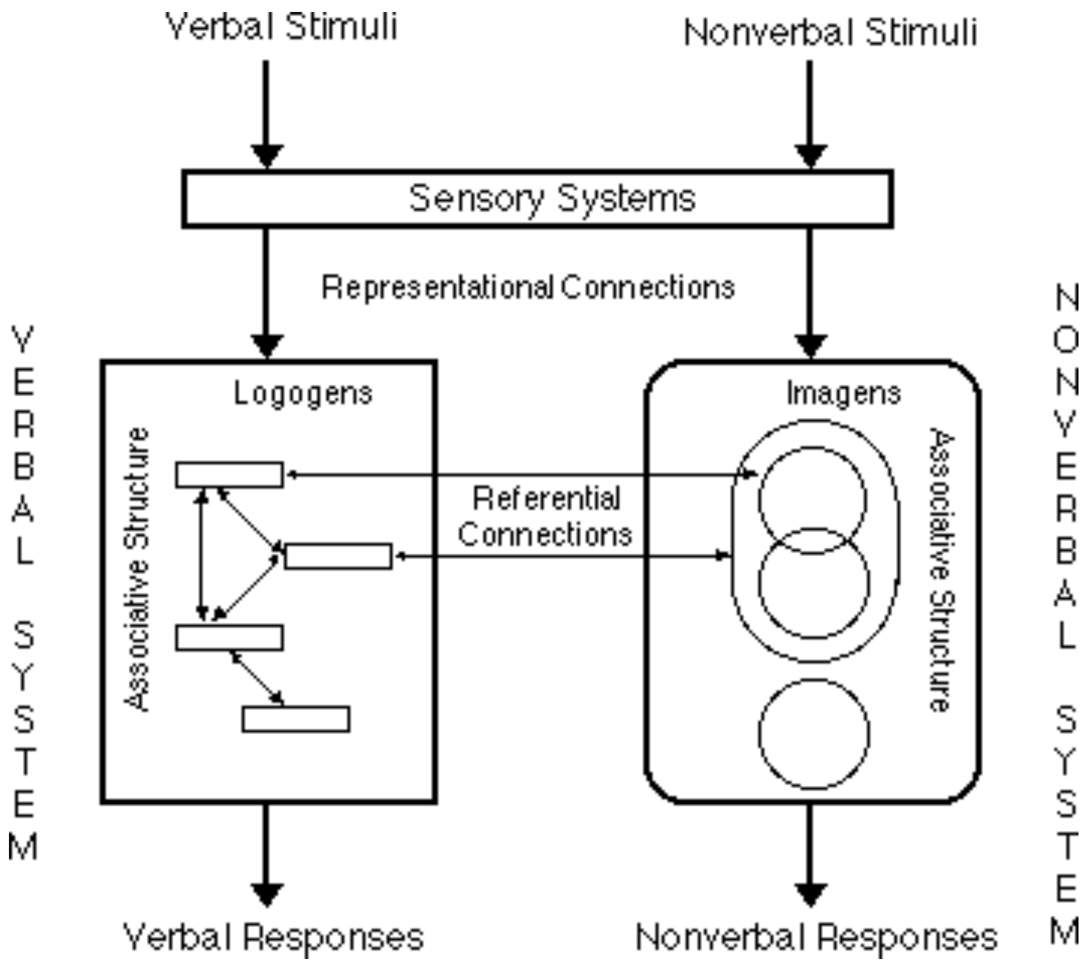
- Blockchain Security and Privacy
- AI Ethics
- Hacking without Humans
- Digital Forensics
- Electronic Voting
- Moving Forward


Privacy in an Era of Drones • Device Physics for Security • Authentication as a Life Skill
IEEE
SECURITY & PRIVACY
Building Dependability, Reliability, and Trust
POSTQUANTUM CRYPTOGRAPHY
PART 2
September/October 2018
Vol. 16, No. 5
Reliability Society
IEEE computer society
IEEE

图形口令简介

使用图形作为口令构成元素

心理学基础



Dual Coding Theory

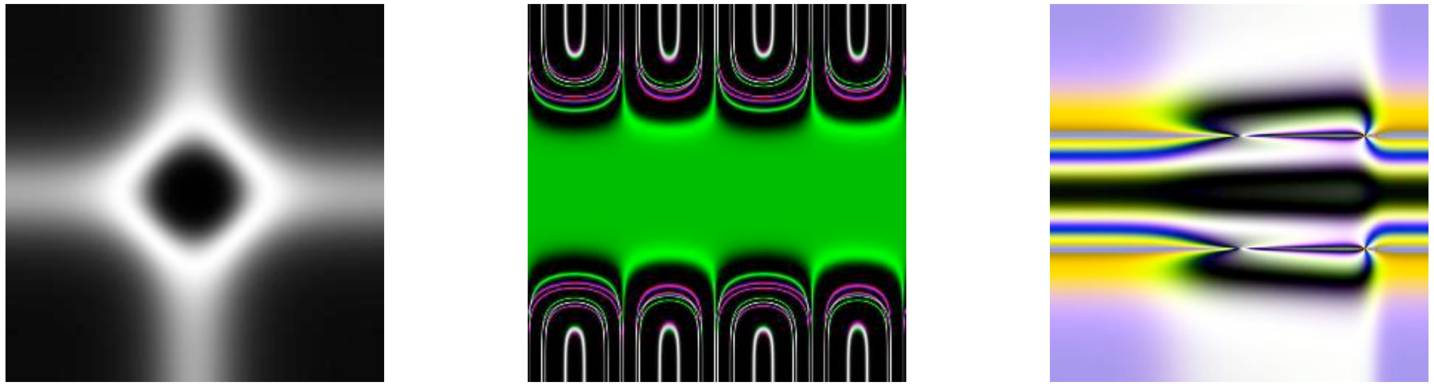
- Recall
- Recognition
- Cued Recall

Recognition is an easier memory task than recall

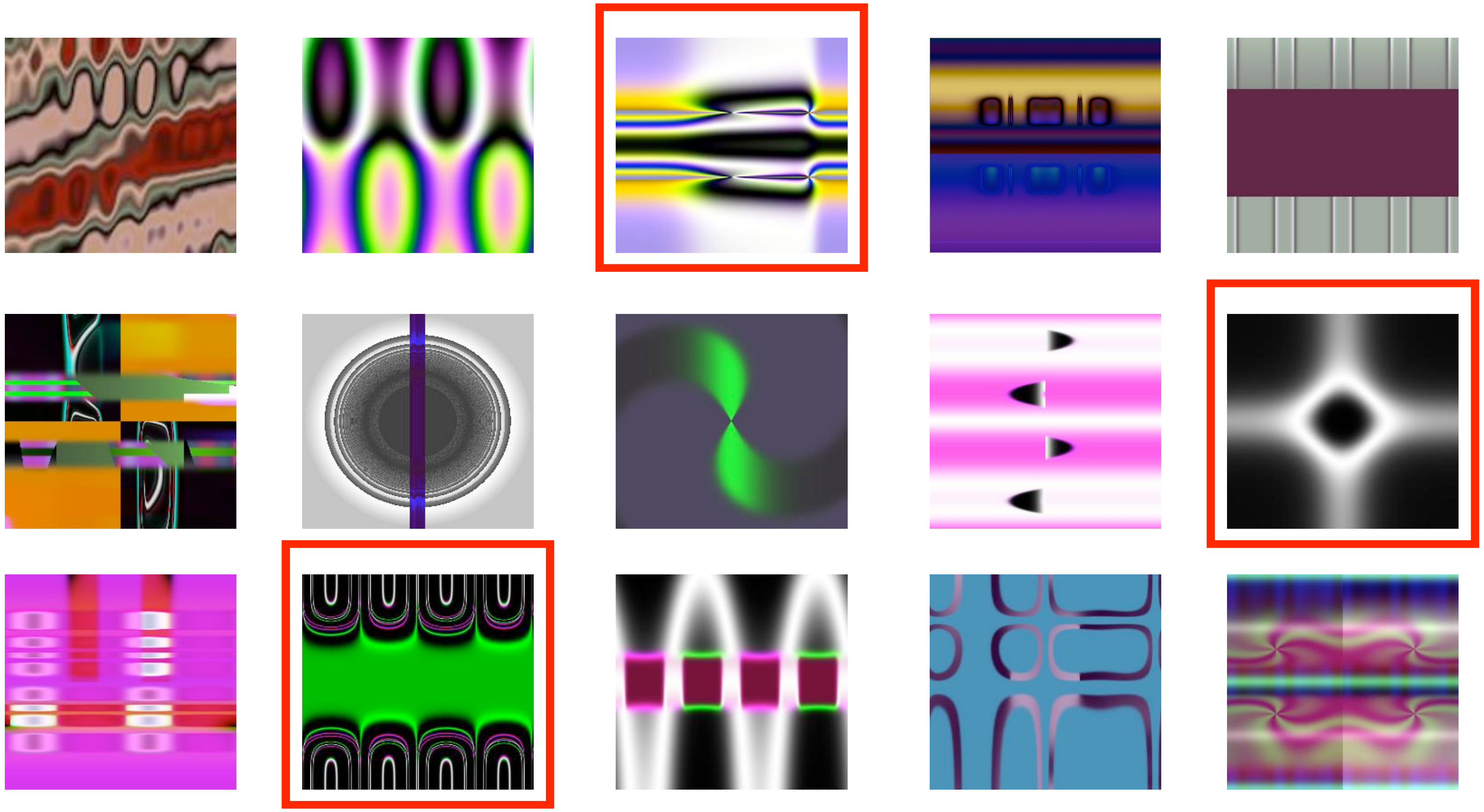
With the aid of a retrieval cue, more information can be retrieved

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）

Pass-Go

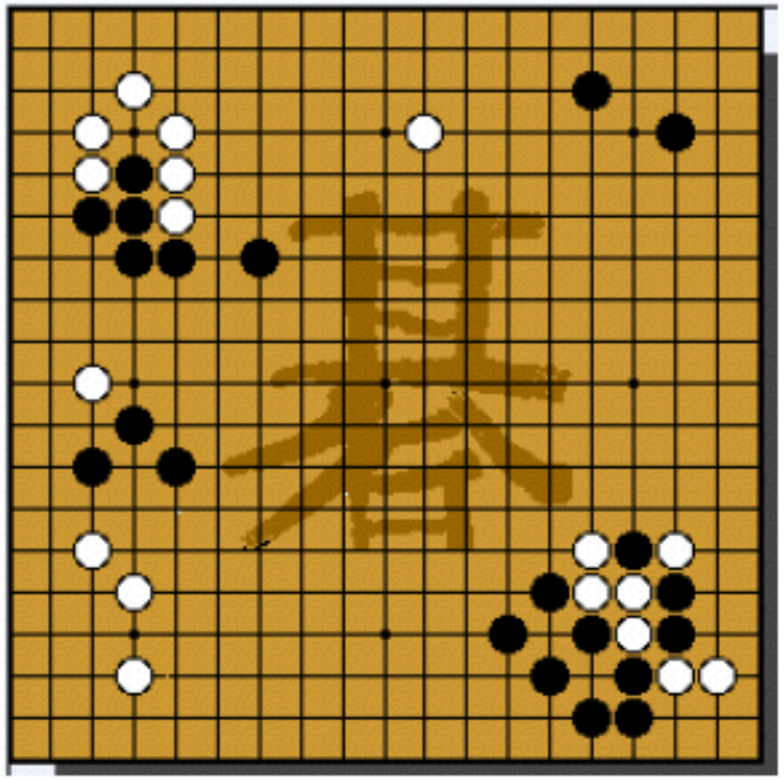


Figure 1 Go game

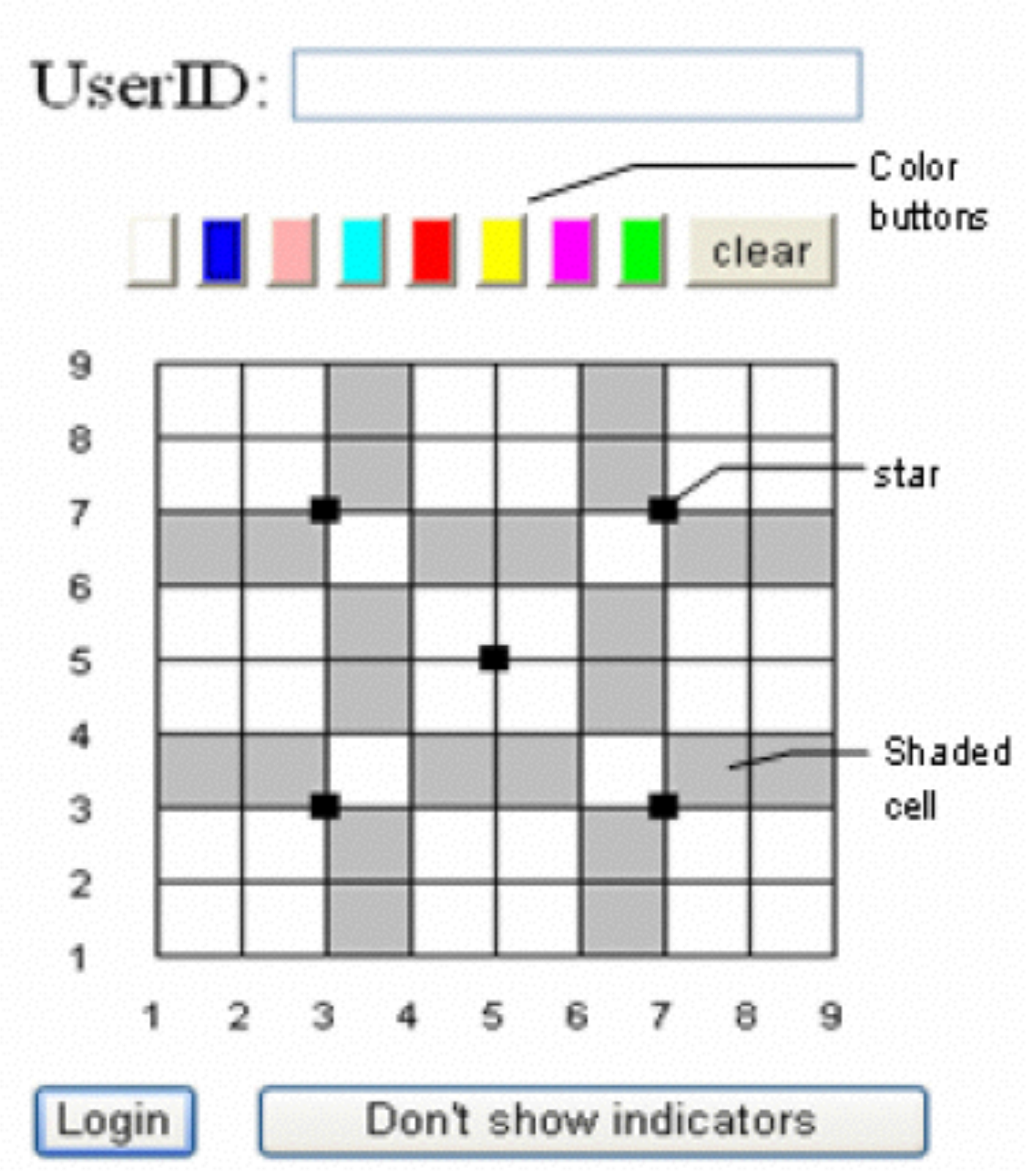
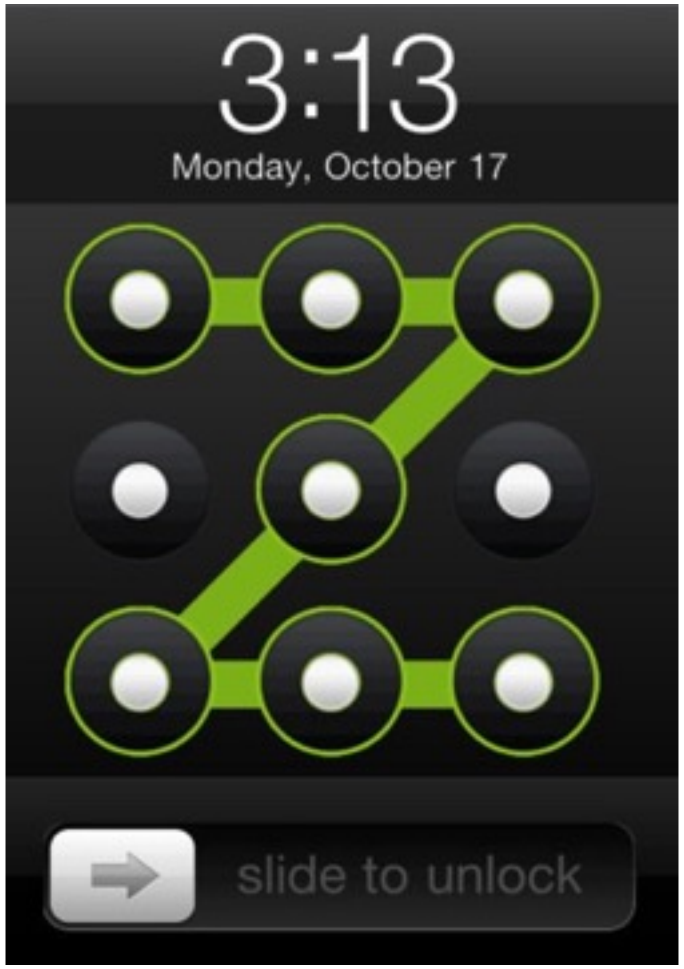
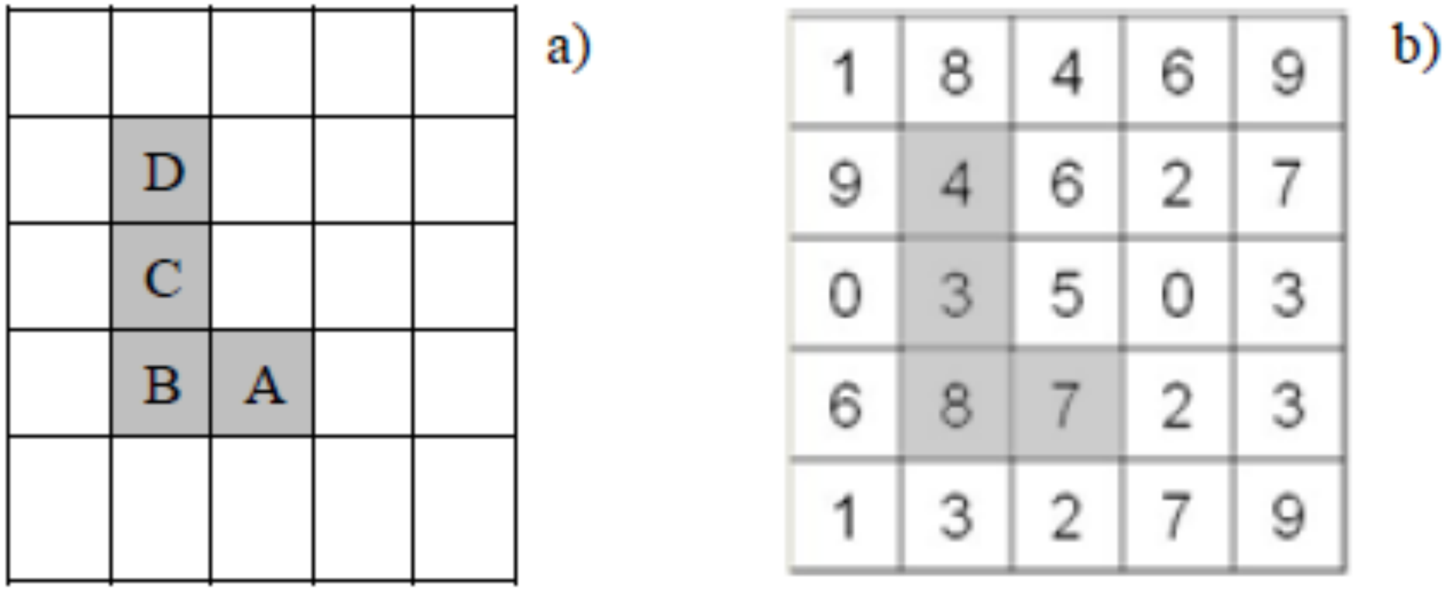


Figure 22 Main login interface

代表产品



PatternLock


a)

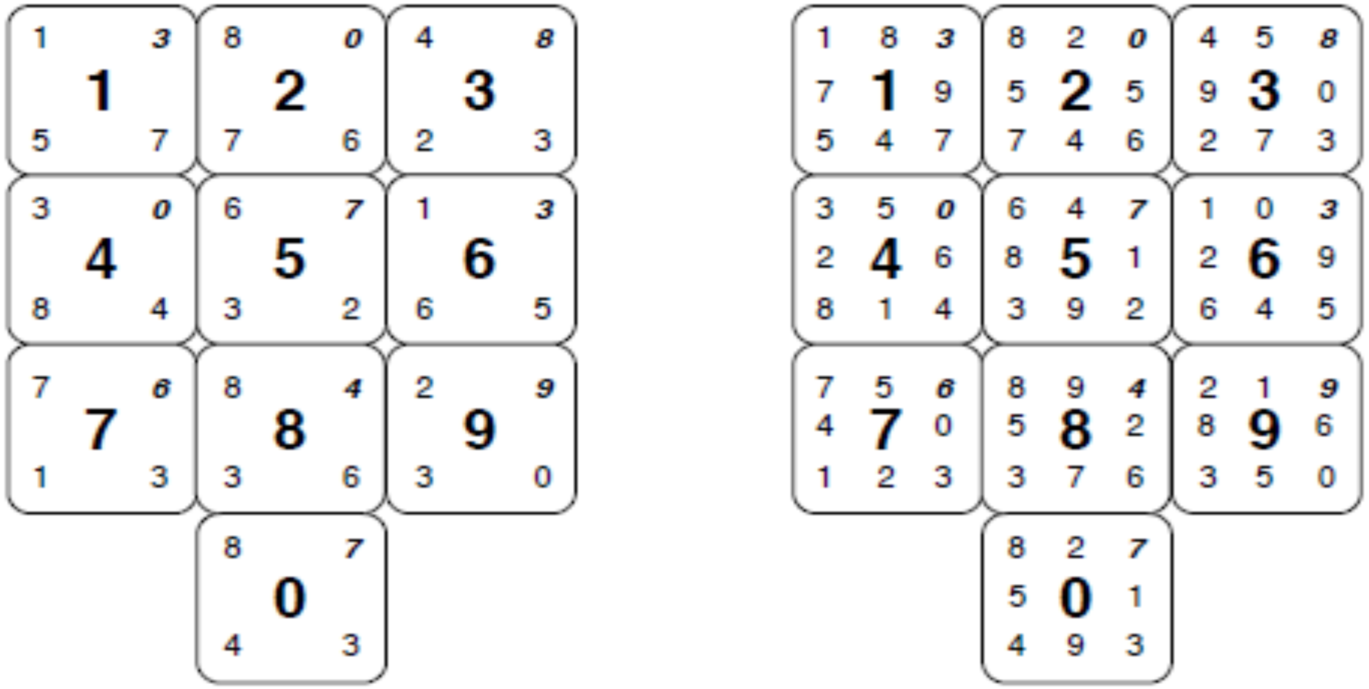
	D			
	C			
	B	A		

b)

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

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



(a) $k = 4$

(b) $k = 8$

GridCode

图形口令分类

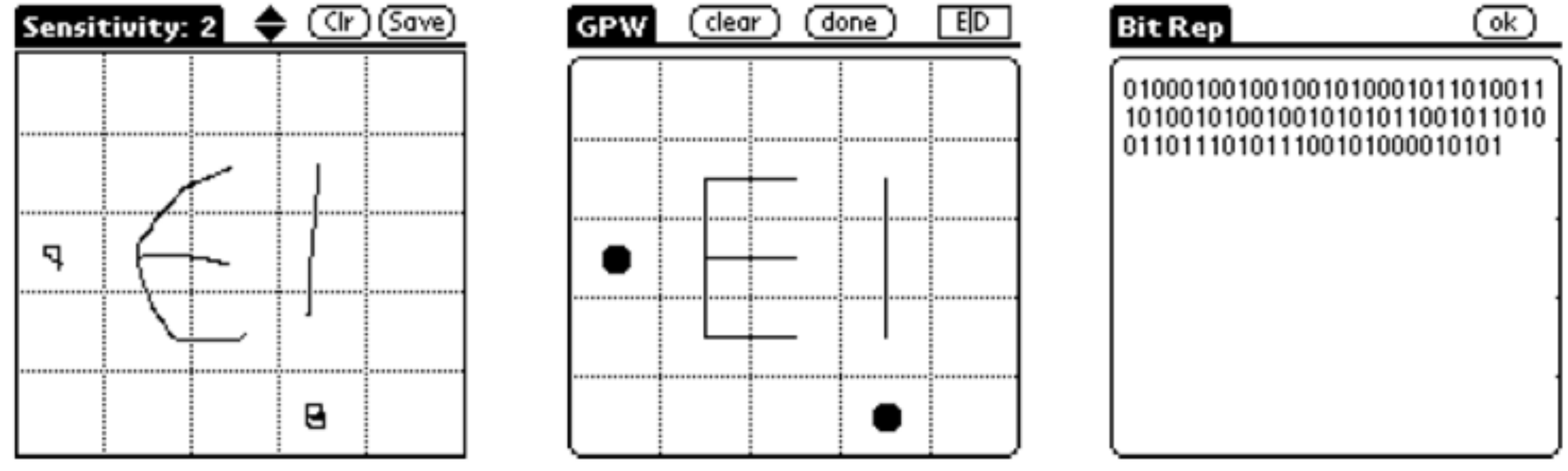
回忆、识别、线索回忆

DAS: Draw-A-Secret

对称图像

很少笔画

中心放置

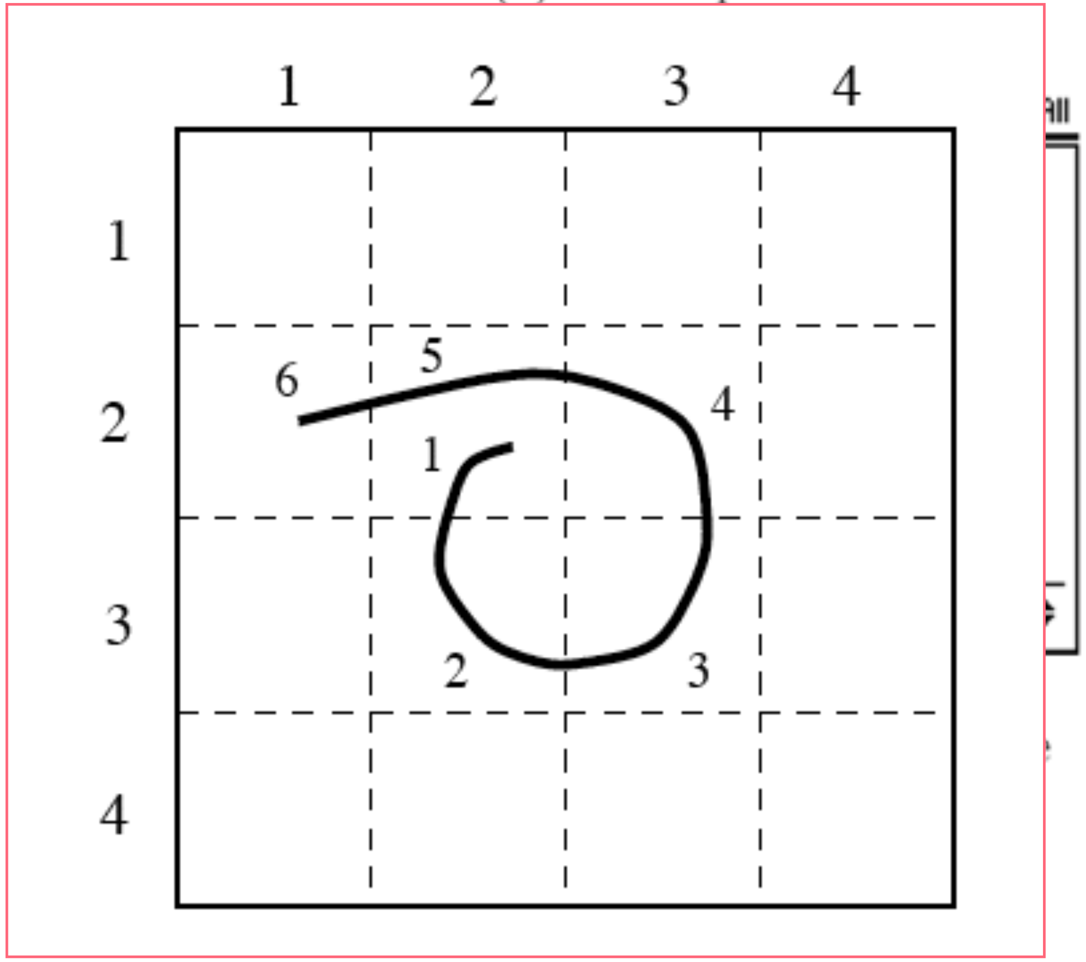


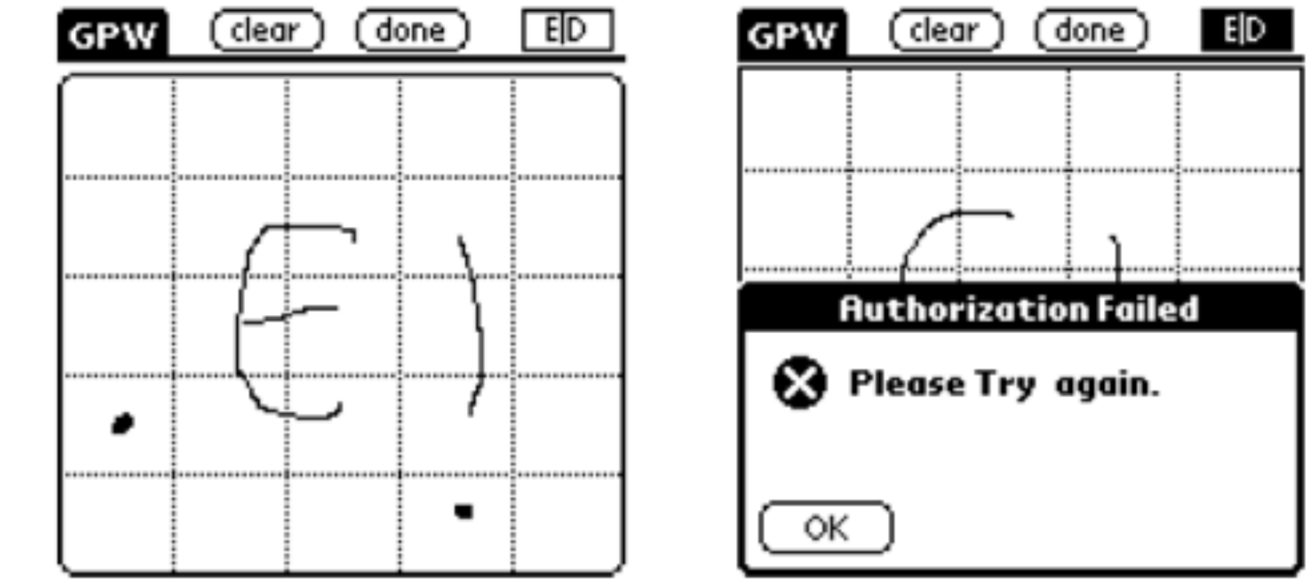
010001001001001010001011010011
101001010010010101011001011010
011011101011100101000010101

(a) User inputs desired secret

(b) Internal representation

(c) Raw bit string





Authorization Failed

Please Try again.

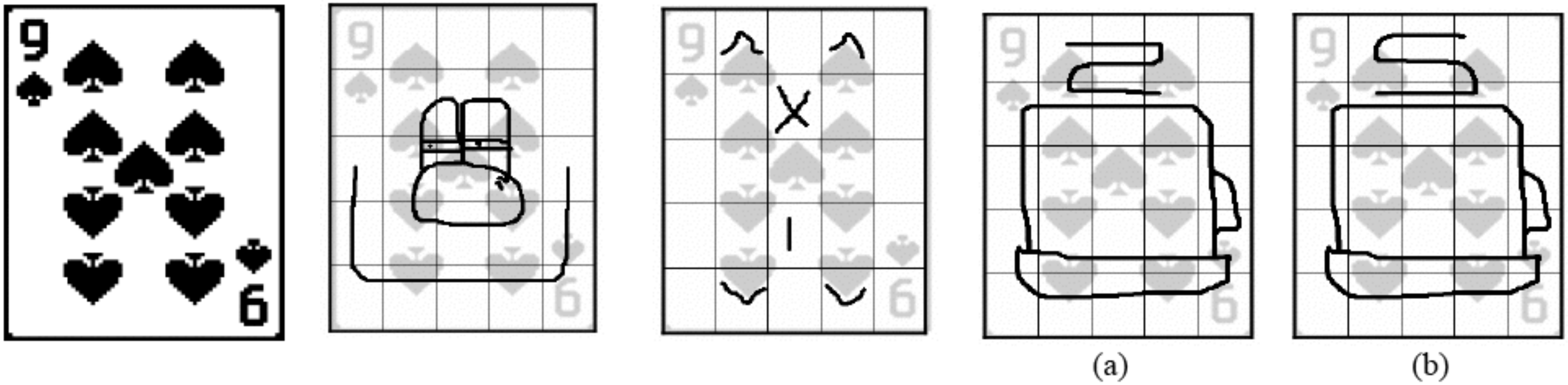
OK

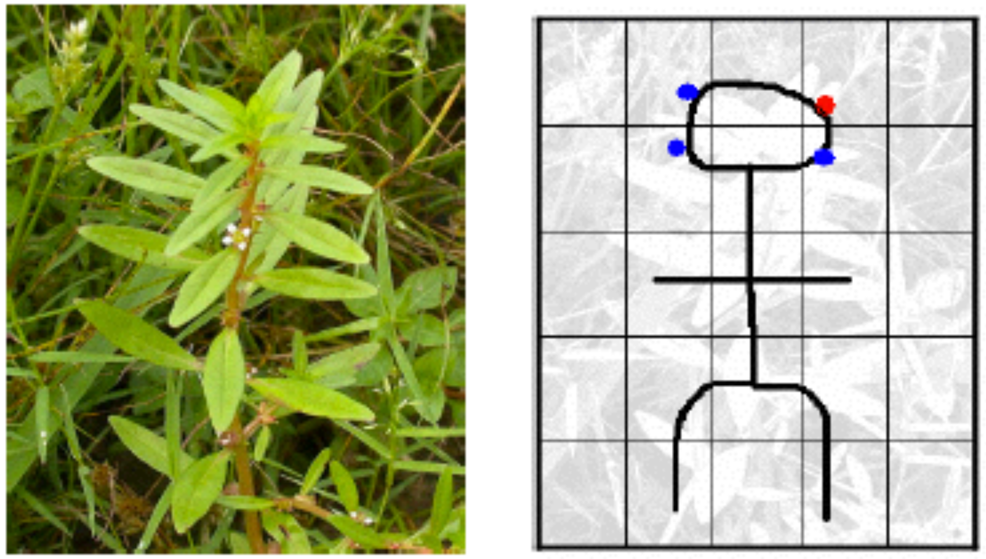
(e) Re-entry of (incorrect) secret

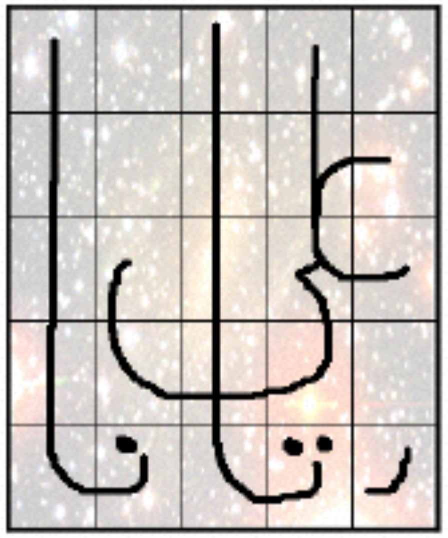
(f) Authorization failed

Recall-Based

BDAS: Background DAS


(a)
(b)





YAGP: Yet Another Graphical Password

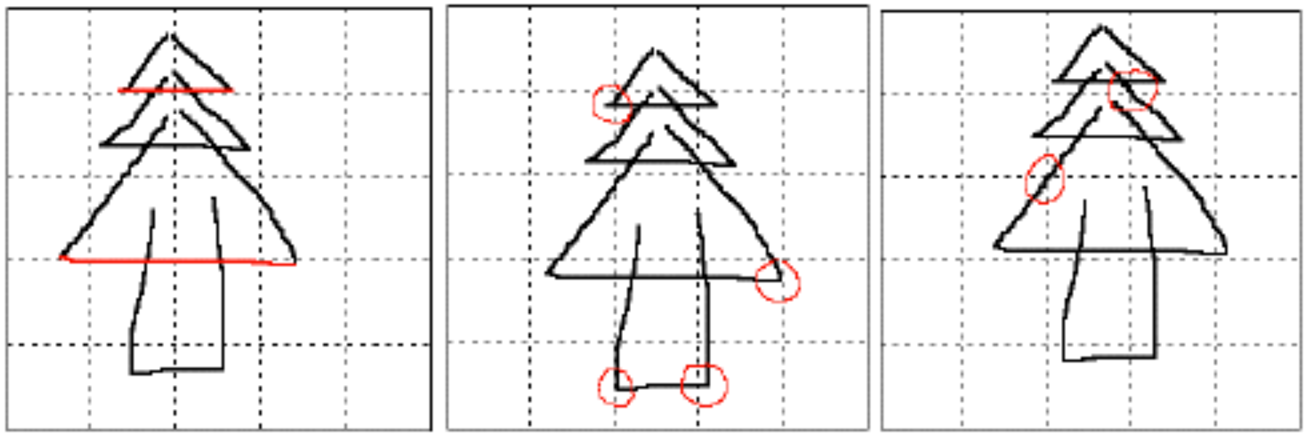
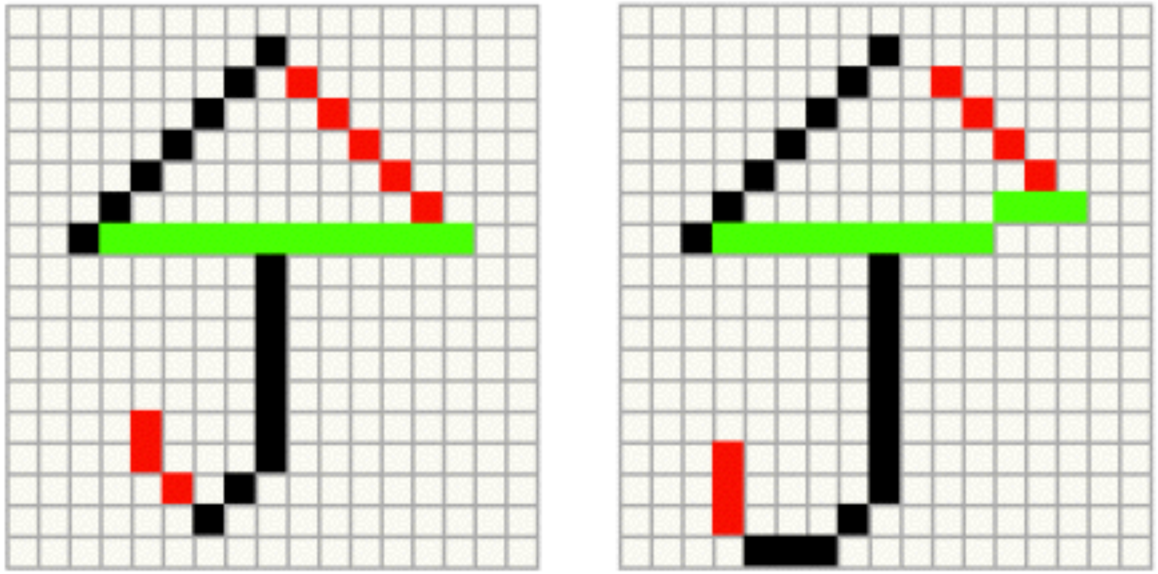
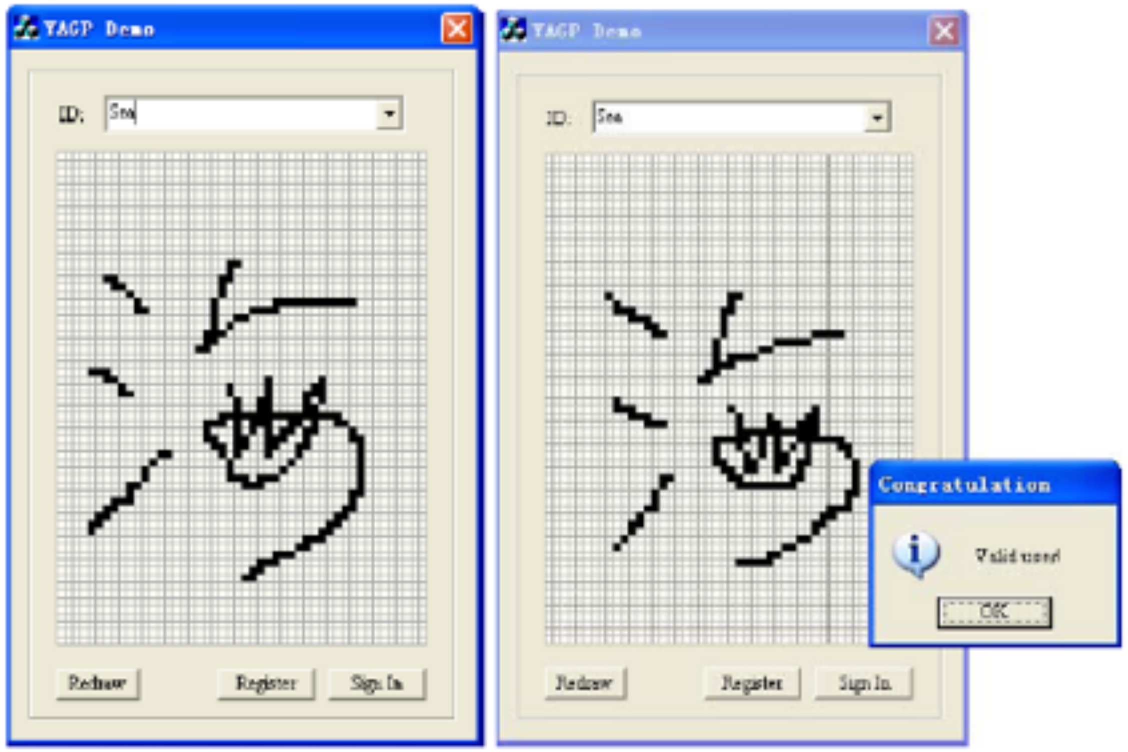

(3.a) (3.b) (3.c)

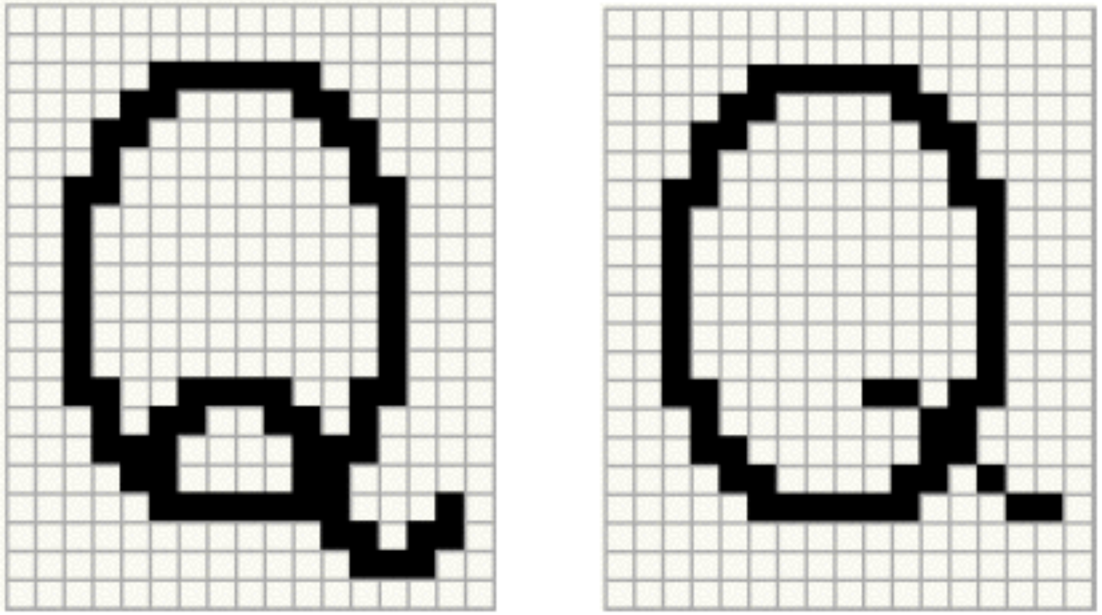
Figure 3. Examples of rule violations in DAS. (a) Lines near grid line. (b) Endpoints near grid line. (c) Strokes near cell corner.


(13.a) (13.b)

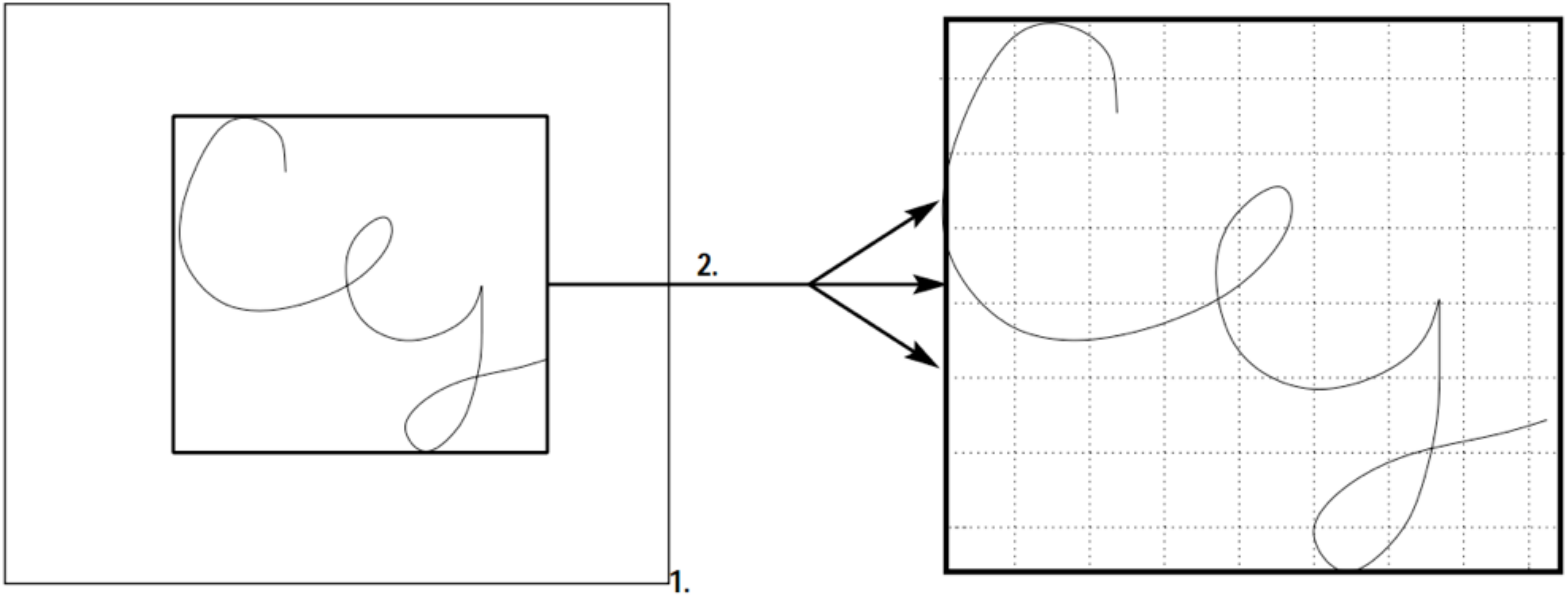


Valid user!

Figure 15. The YAGP system Interface (48×64 density grid).


(11.a) (11.b)

Passdoodle



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 accross distribution grid
   - Compare instantaneous speed
4. If tests confirm identify of user, authenticate, if not repeat analysis agianst other stored users.

4. If tests confirm identify of user, authenticate, if not repeat analysis agianst other stored users.

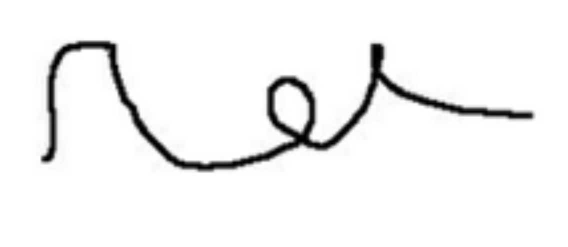
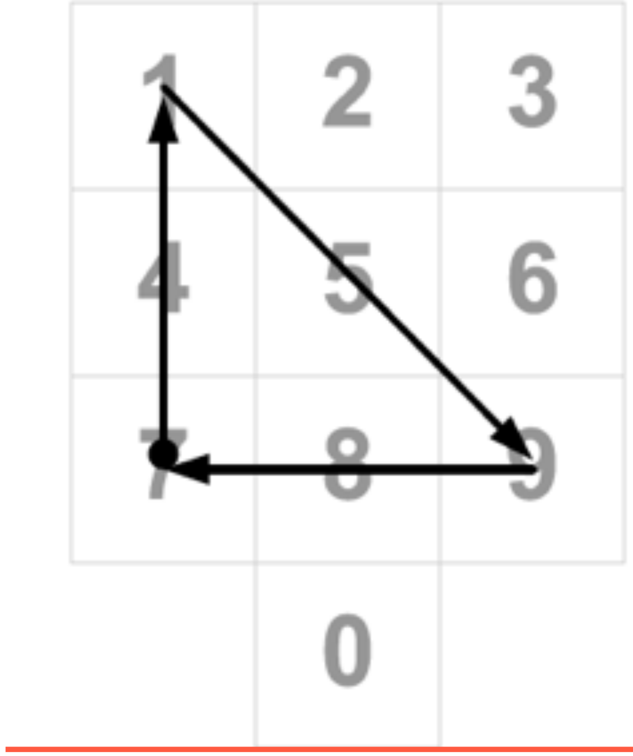


Figure 1: An Example of a Passdoodle

PassShapes



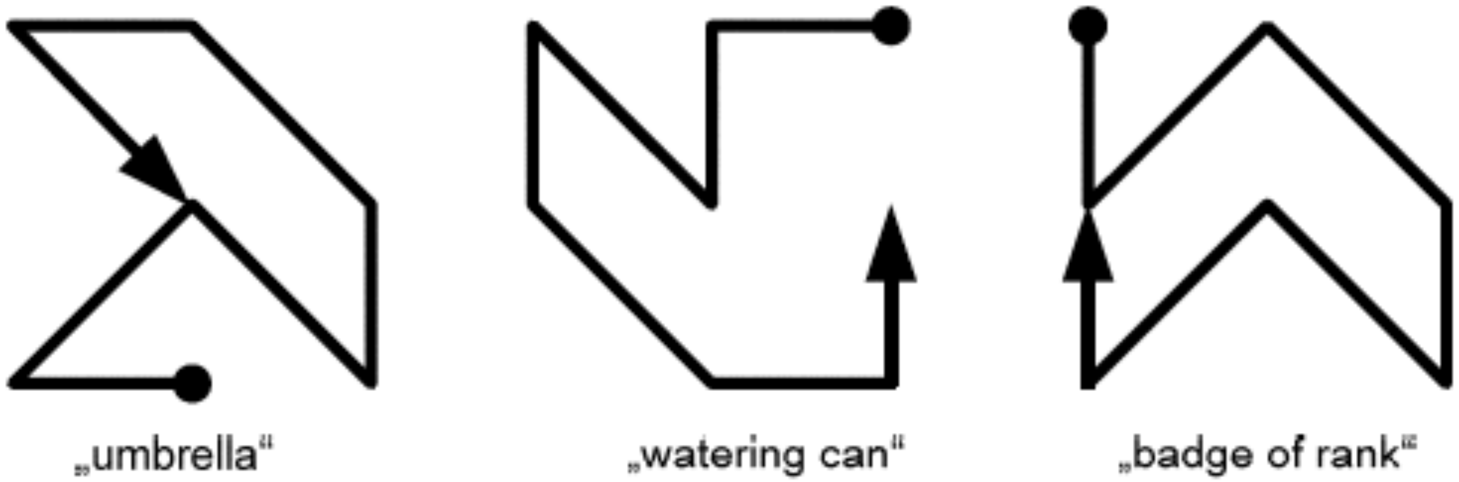


Figure 6: PassShapes and users' associations

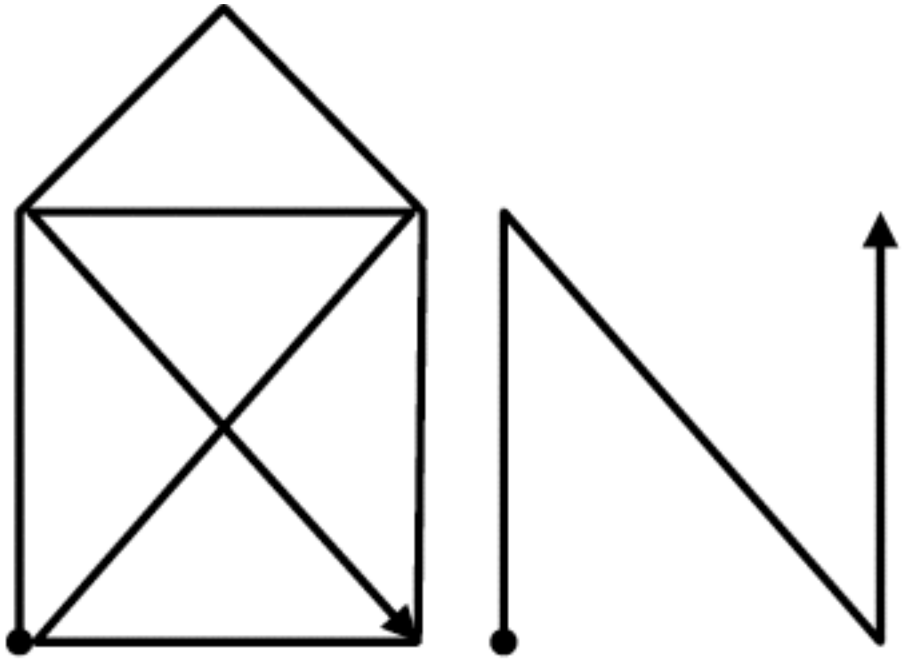
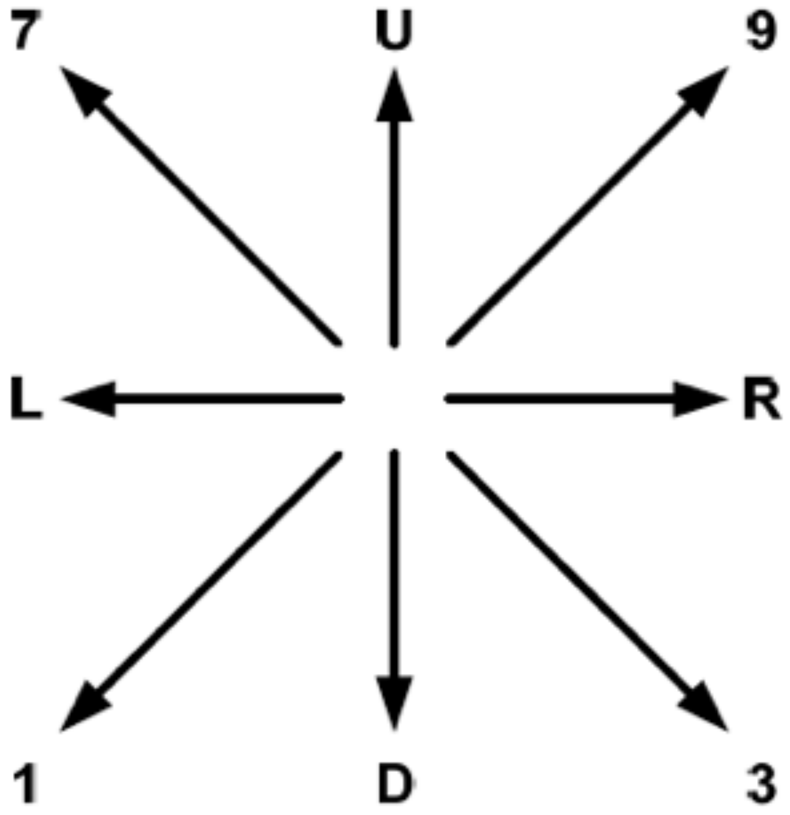


Figure 3: An example PassShape with the internal representation U93DL9L3XU3U



Pass-Go

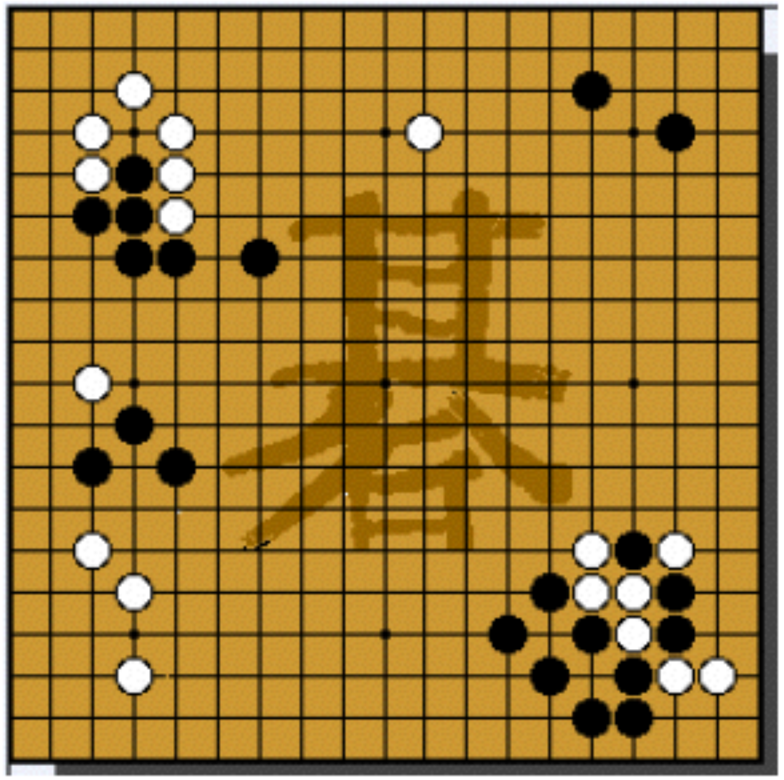


Figure 1 Go game

扩展：测量压力

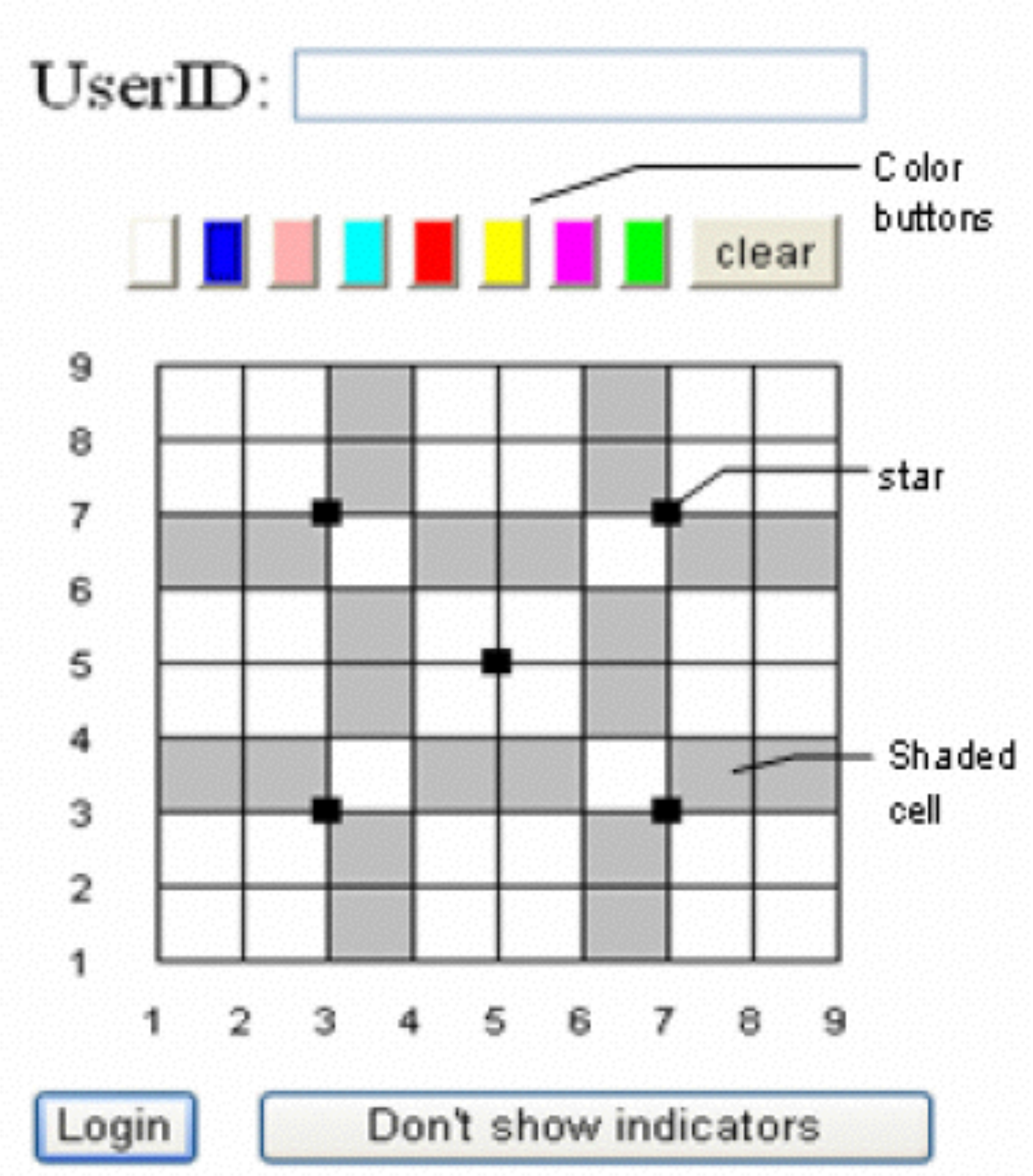


Figure 22 Main login interface

Deja Vu

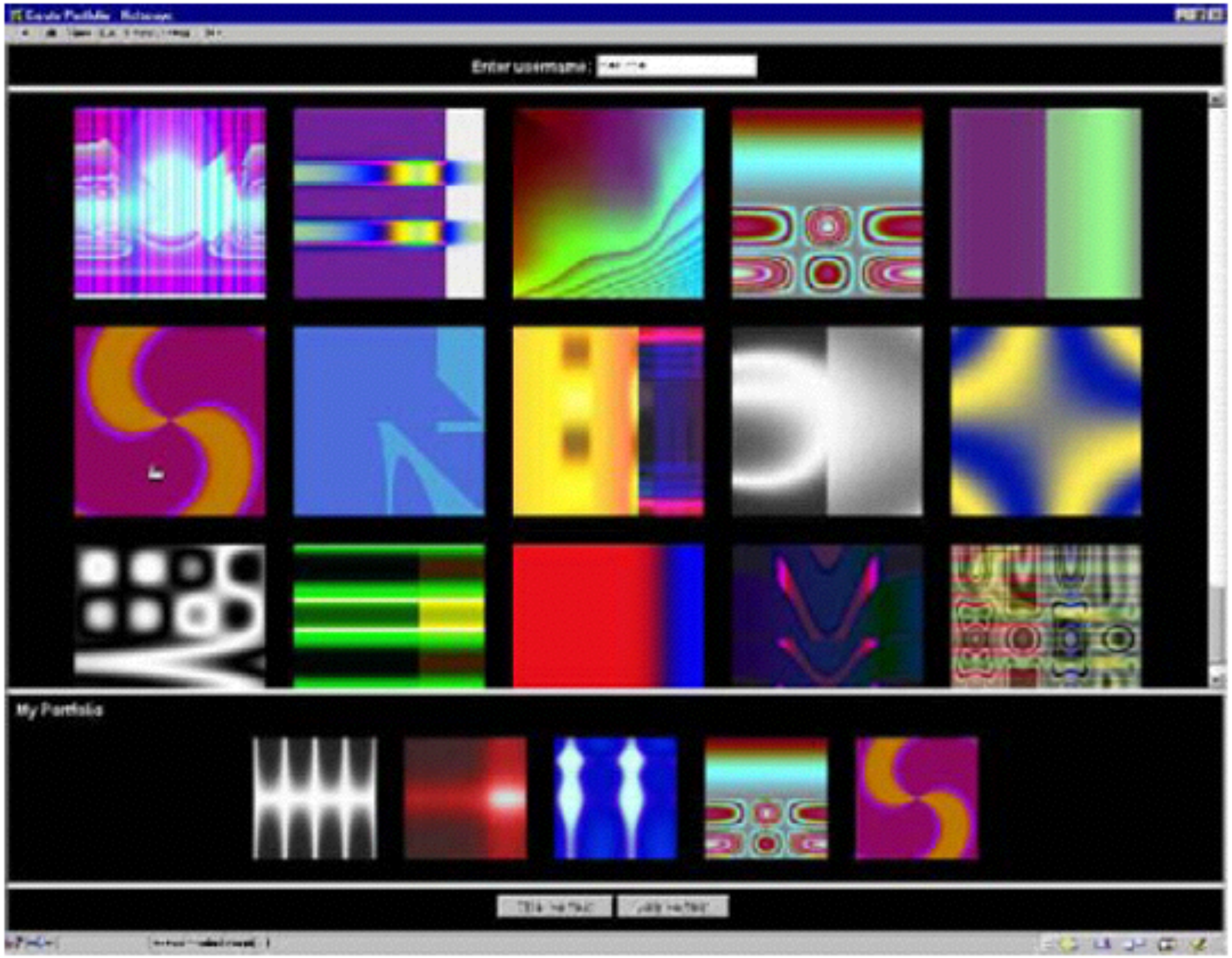


Figure 8 Déjà Vu [Dhamija and Perrig 2000]

PassFaces

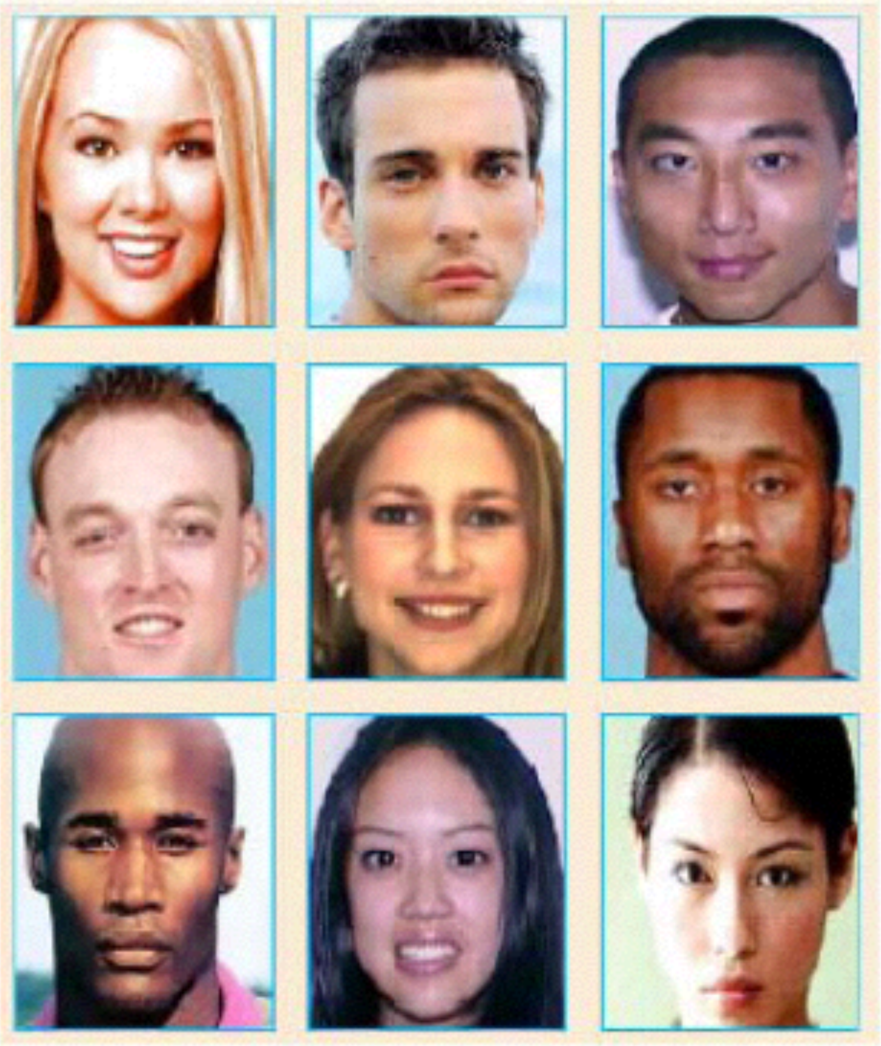


Figure 6 Passfaces$^{\text{TM}}$ [Passfaces 2006]

- 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

Story

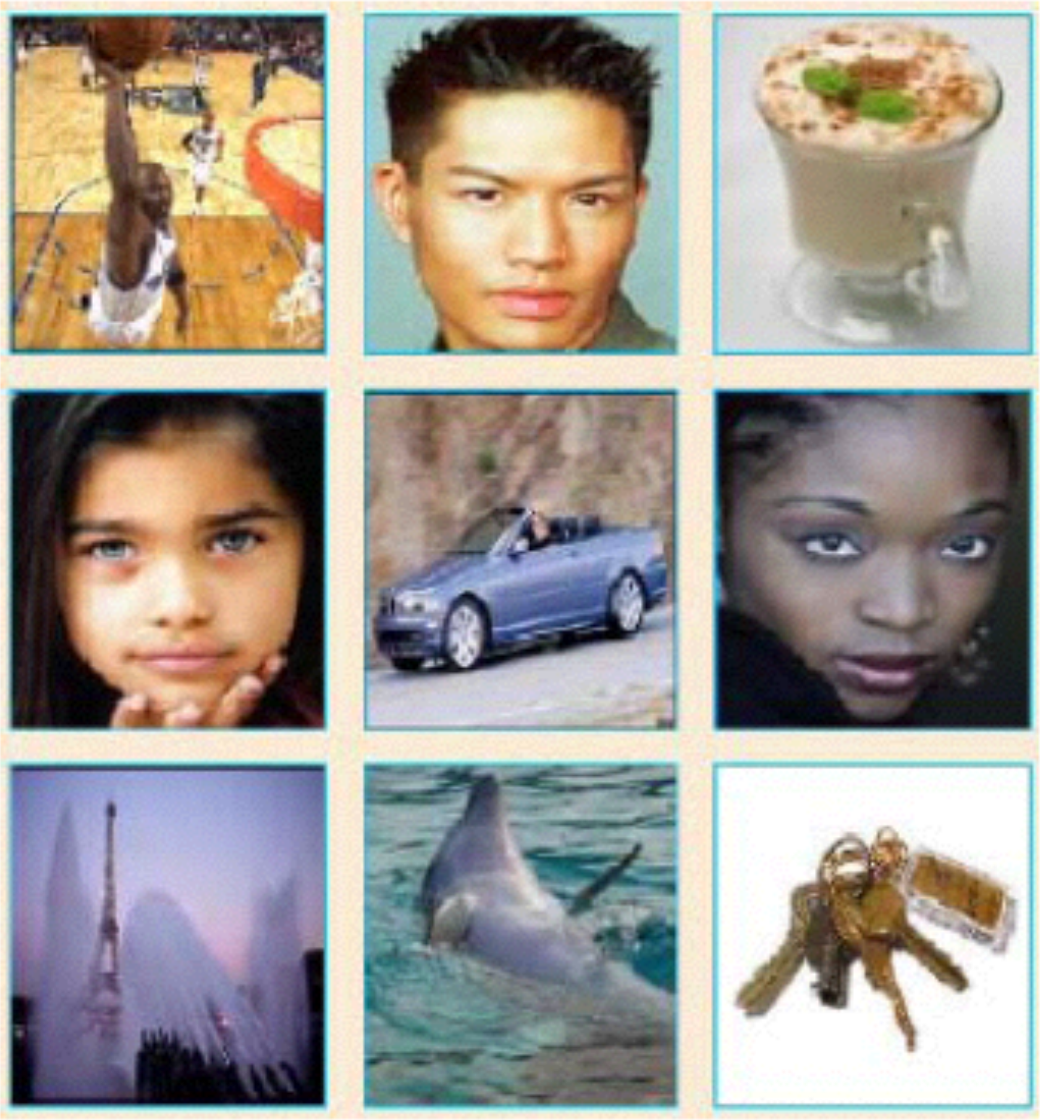
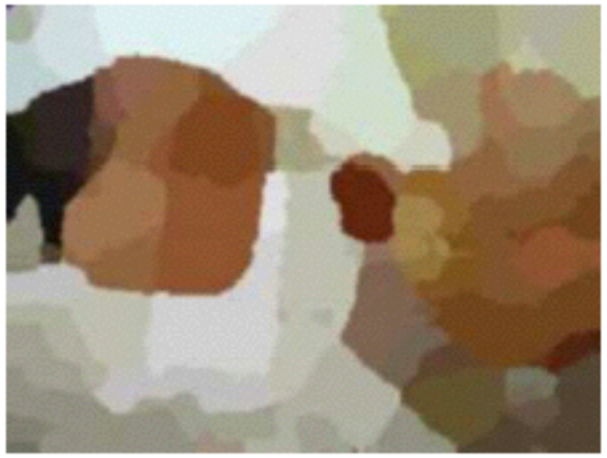


Figure 7 Story scheme [Davis et al. 2004]

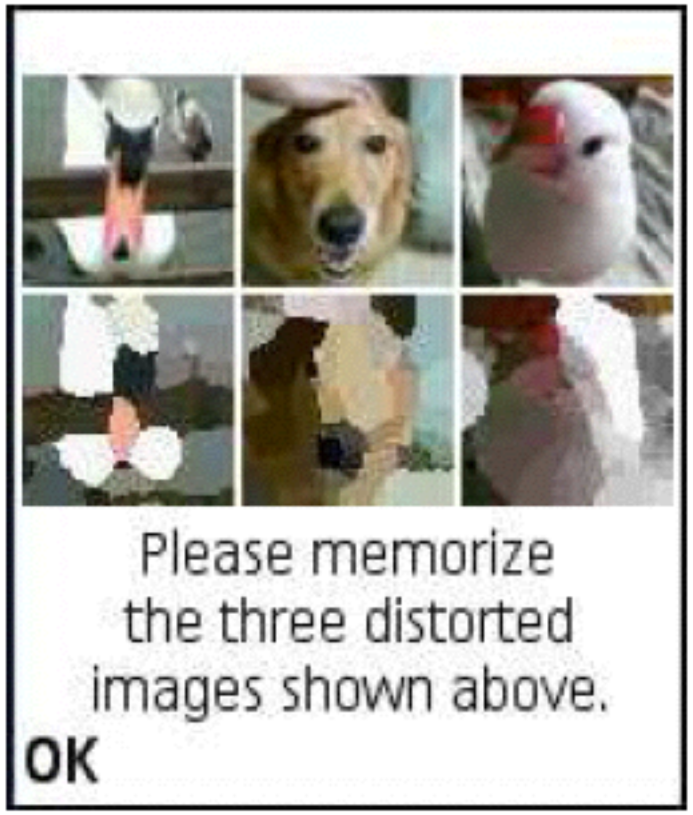
- 图像之间有序
- 口令空间更大
- 记忆有负担

Use your Illusion

可用性干扰

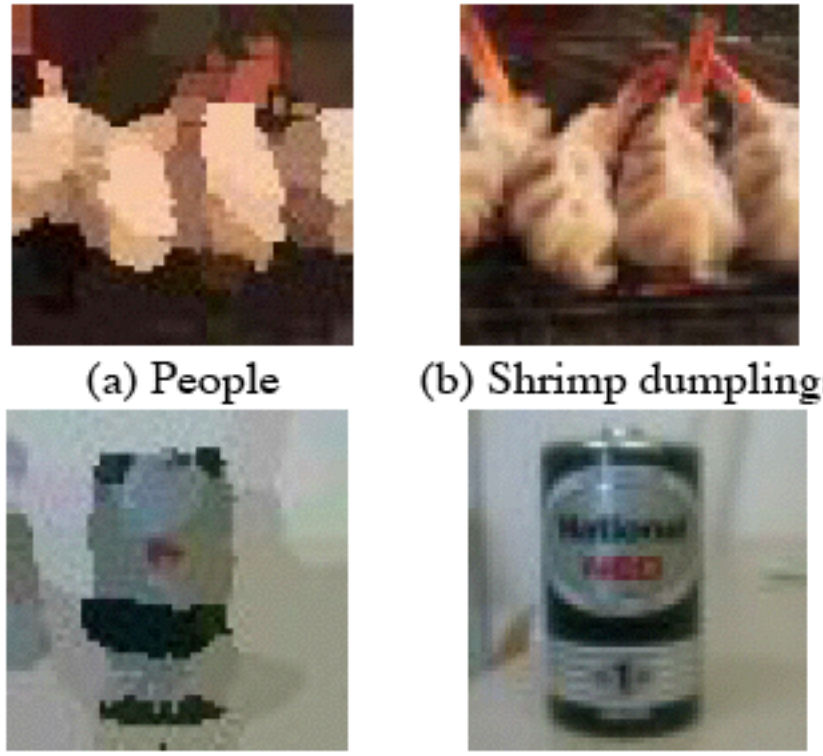


马赛克去除技术



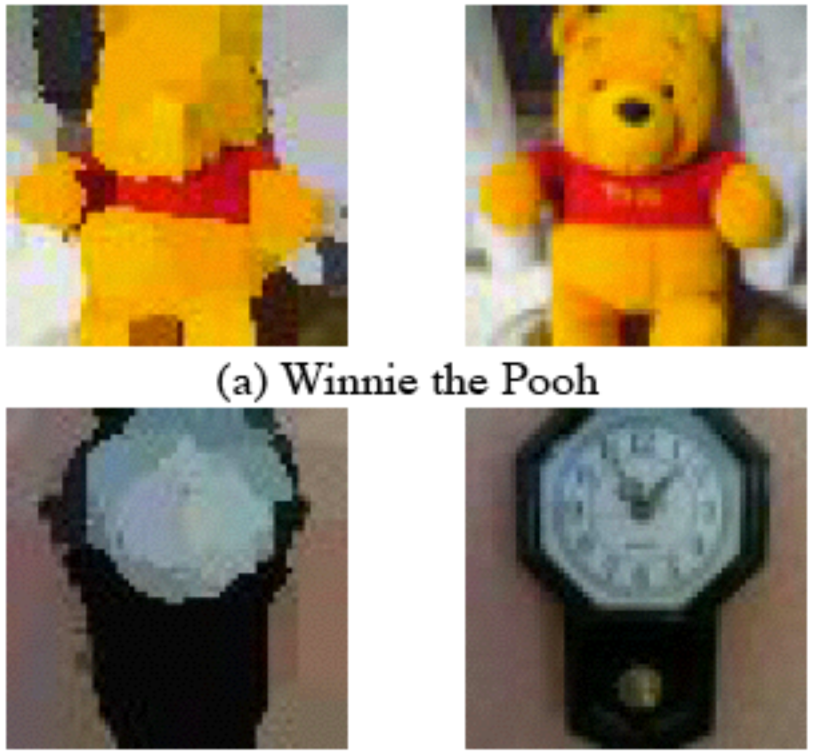
Please memorize the three distorted images shown above.

OK



(a) People (b) Shrimp dumplings

(c) Panda (d) Battery



(a) Winnie the Pooh

(b) Wall Clock

Cued Recall-Based

Passpoints

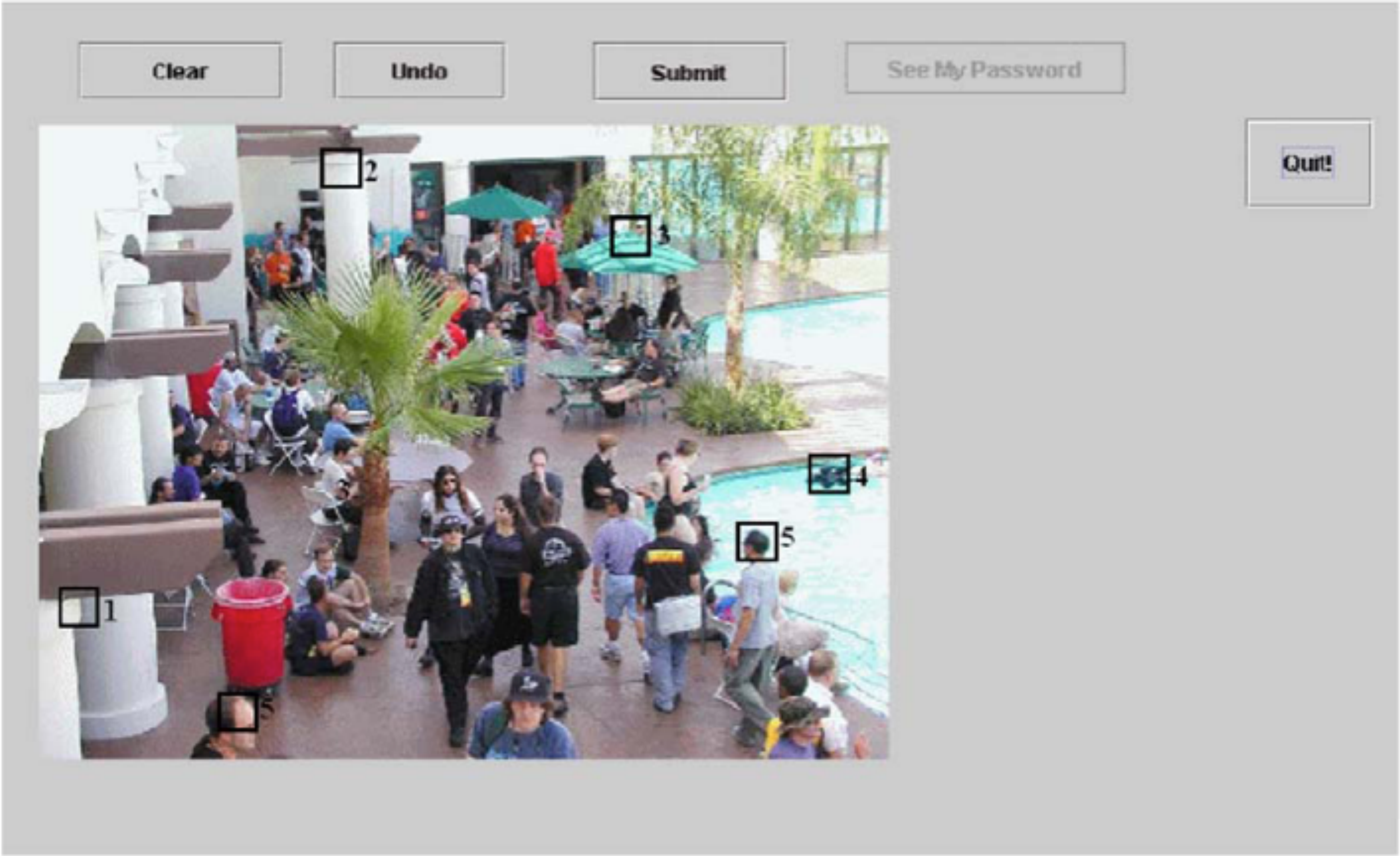


Fig. 2. Example of participant password with tolerance and click order displayed.

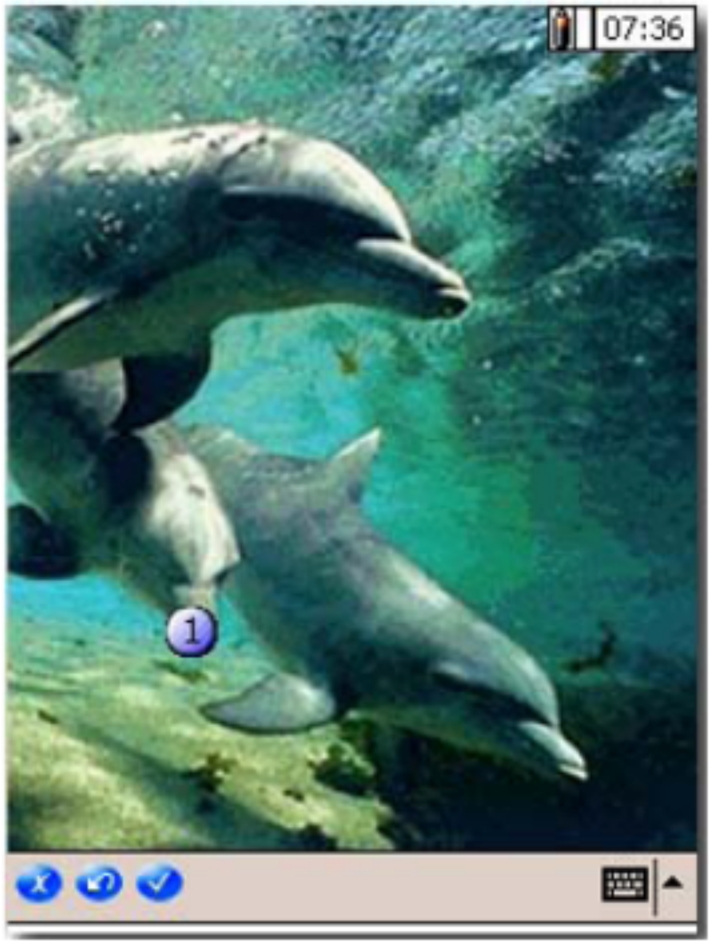


Figure 3 VisKey [Sfr 2006]

- 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

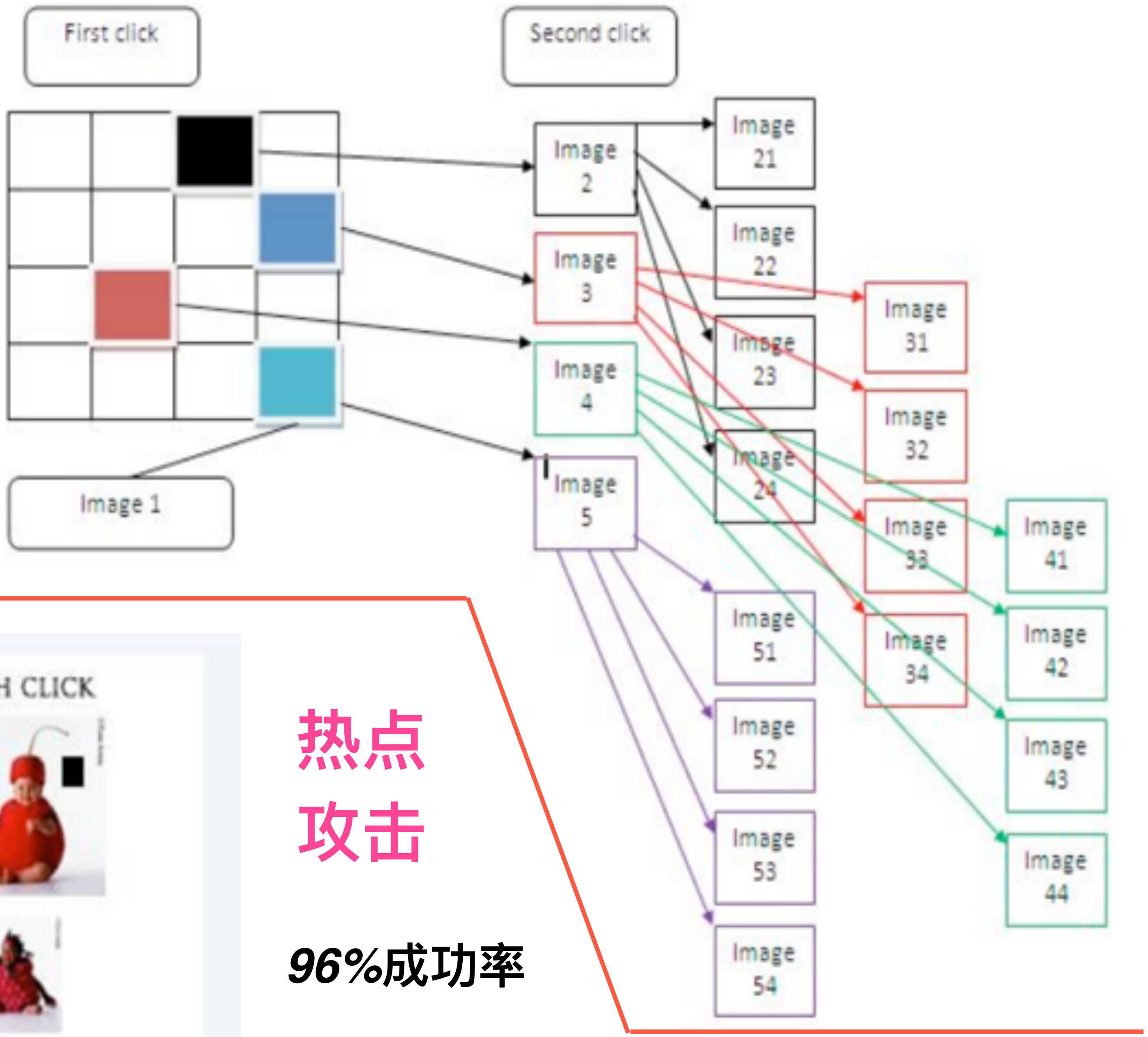
热点攻击

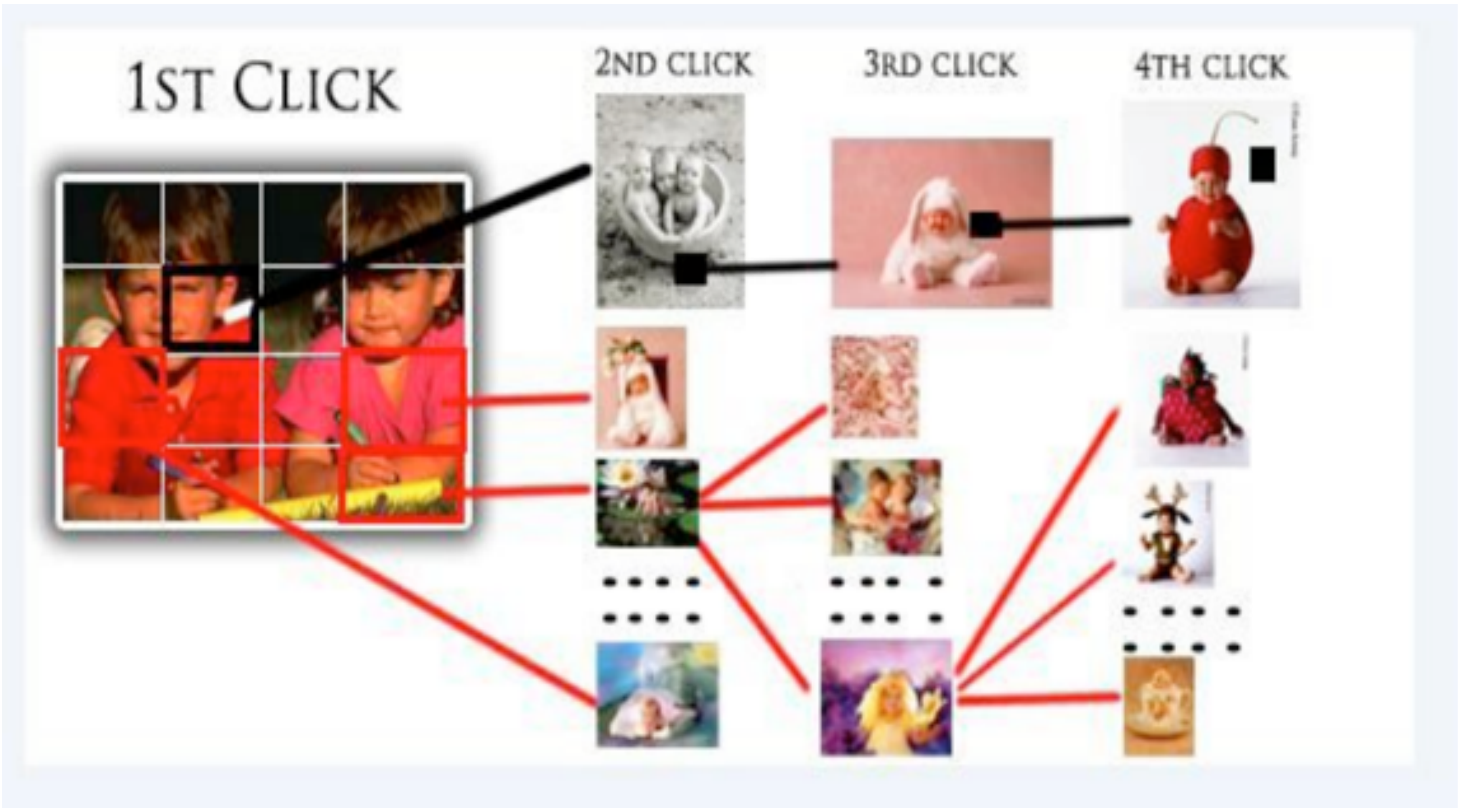
多个口令

一对多

CCP: Cued Click Points

- 一对一线索
- implicit feedback
- 避免简单模式



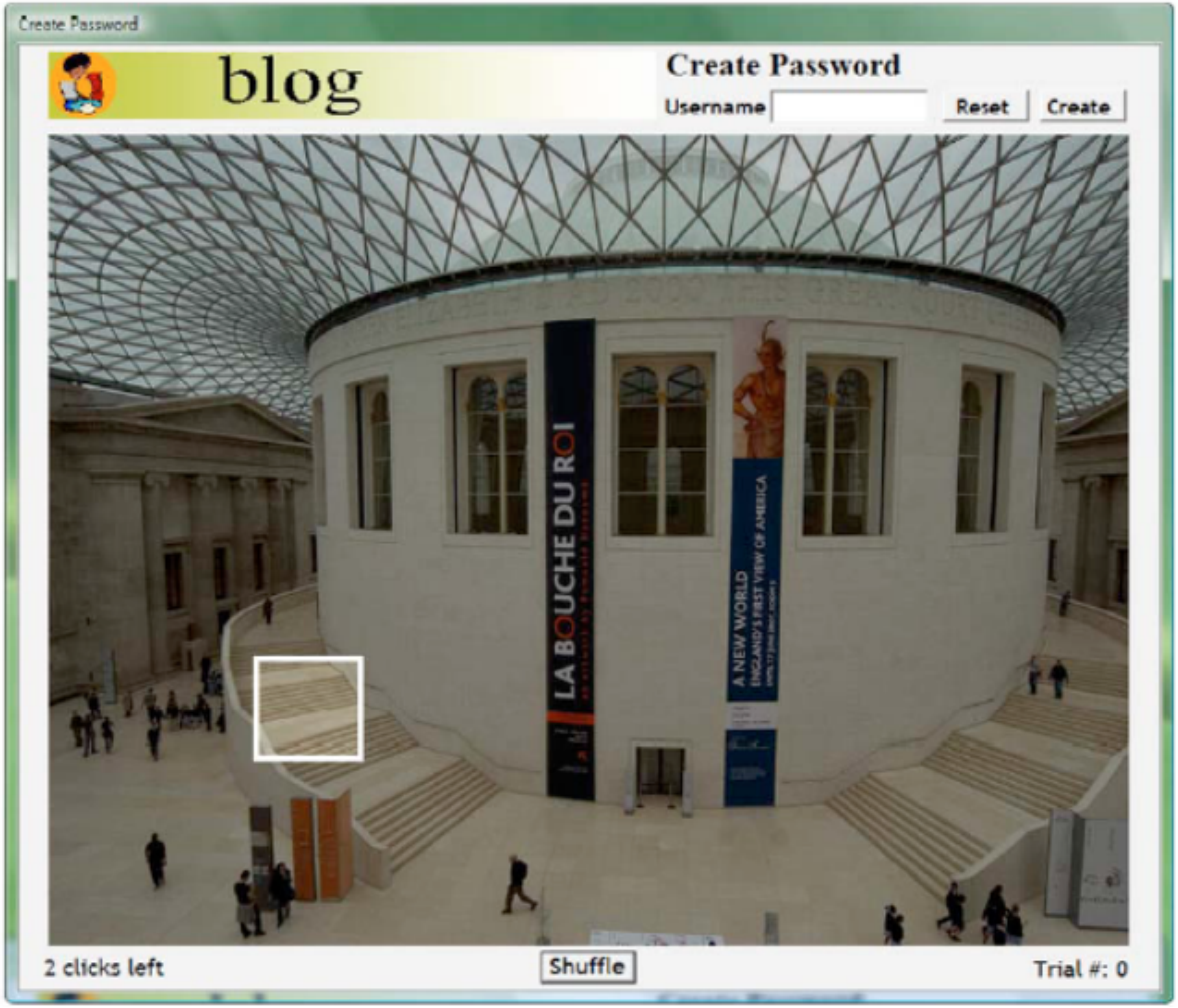


热点
攻击

*96%*成功率

- 注册：25秒
- Login：7秒

PCCP: Persuasive CCP

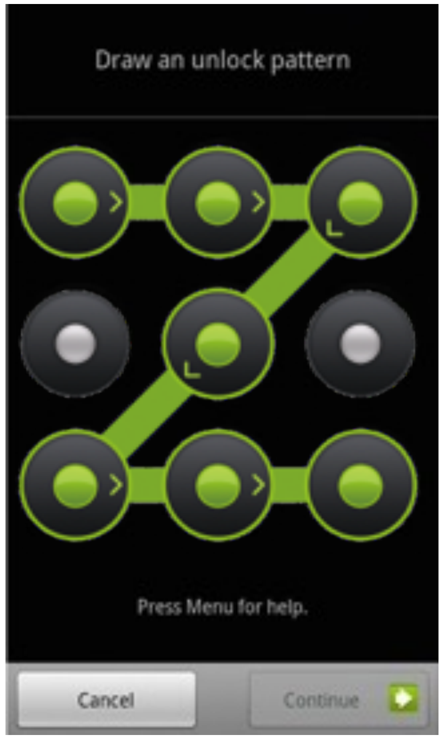


- viewport
- 随机化
- 避免hotspots
- 创建：50秒
- Login：8秒

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*

后备认证

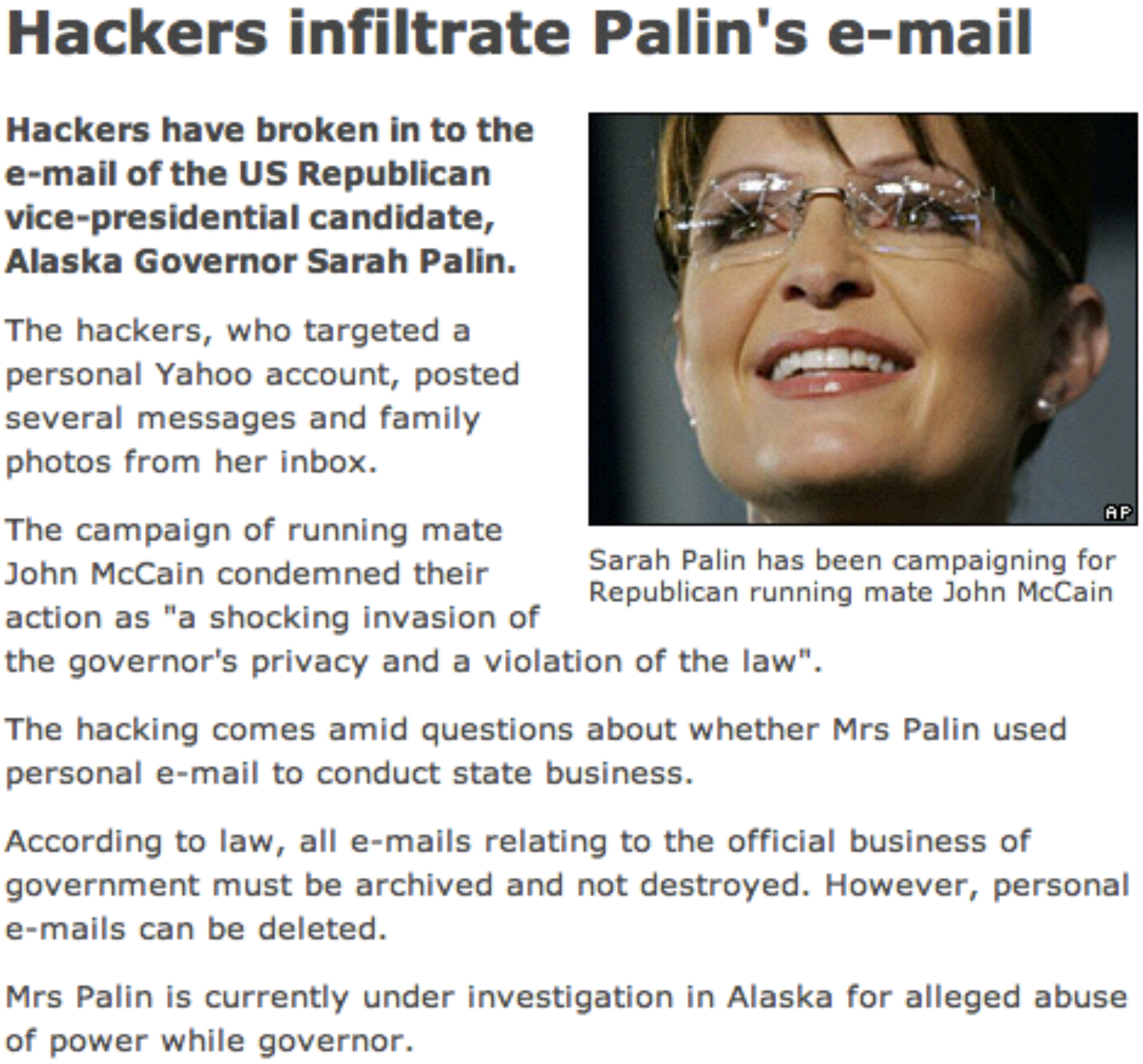
US08 FULL ELECTION COVERAGE

Electoral College votes	Winning post 270
Obama - Democrat	365
McCain - Republican	173

BBC NEWS

2008.09.17

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.

Sarah Palin has been campaigning for Republican running mate John McCain

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.

gov.palin@yahoo.com

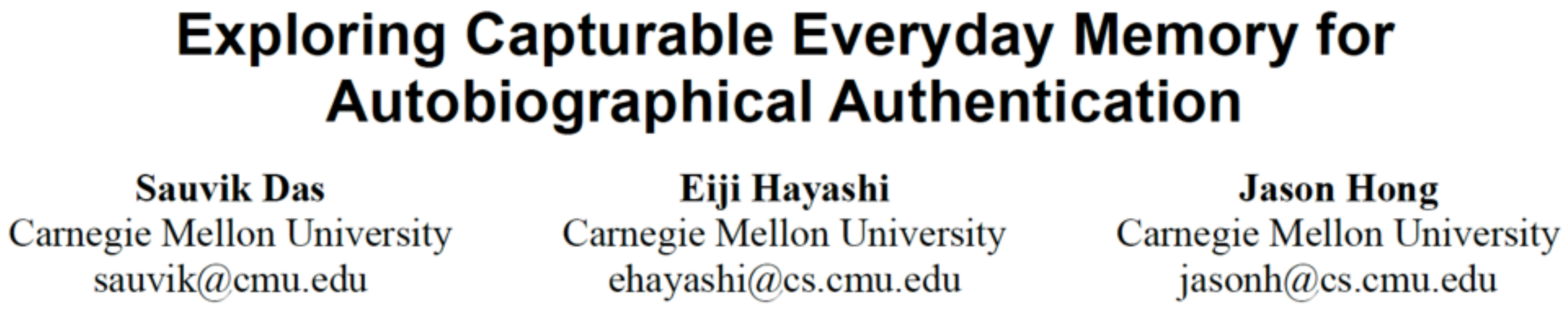
Where did you meet your spouse?

Wasilla High School

http://wikileaks.org/wiki/VP_contender_Sarah_Palin_hacked

2008

自传体认证

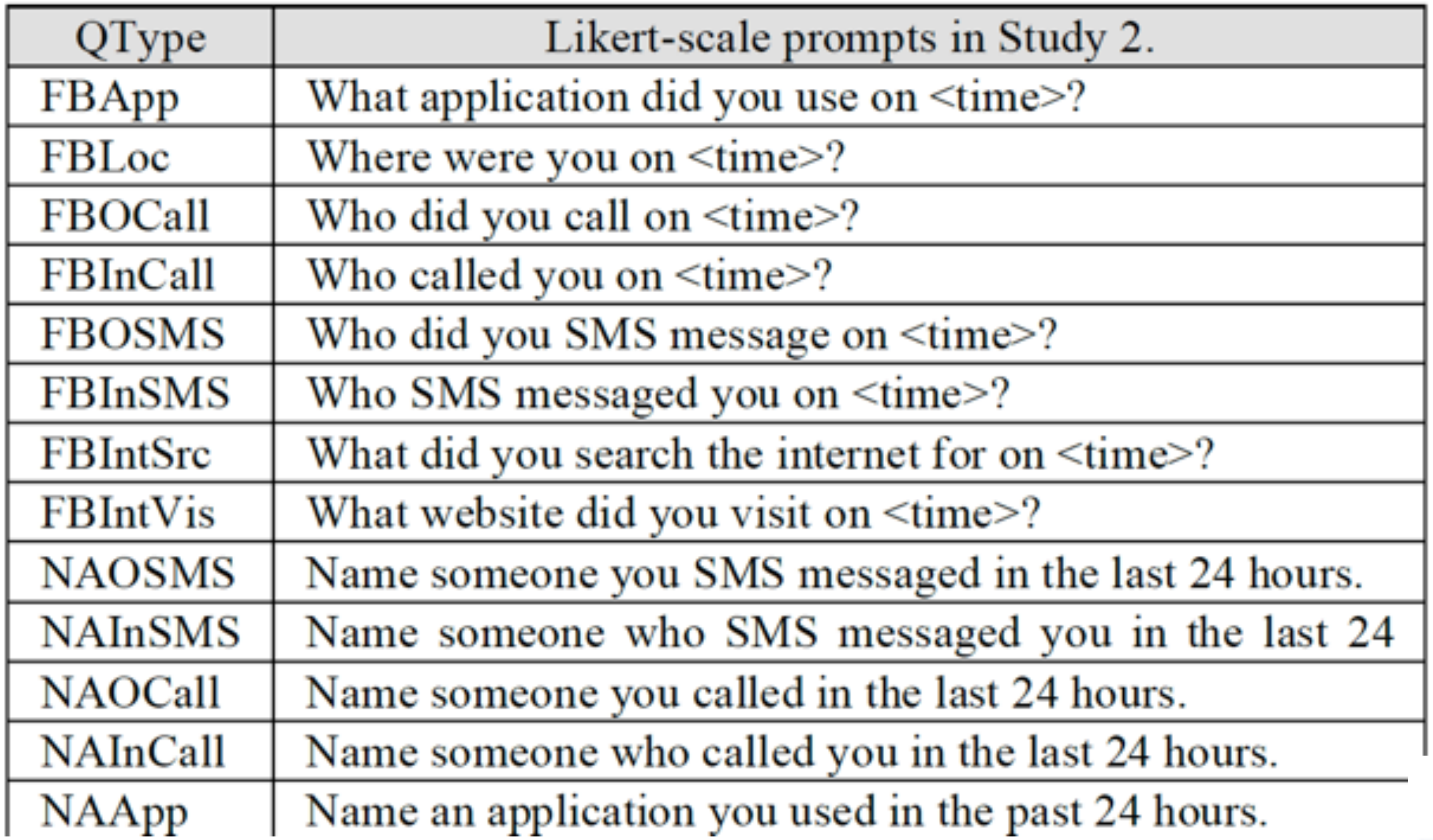


Exploring Capturable Everyday Memory for Autobiographical Authentication

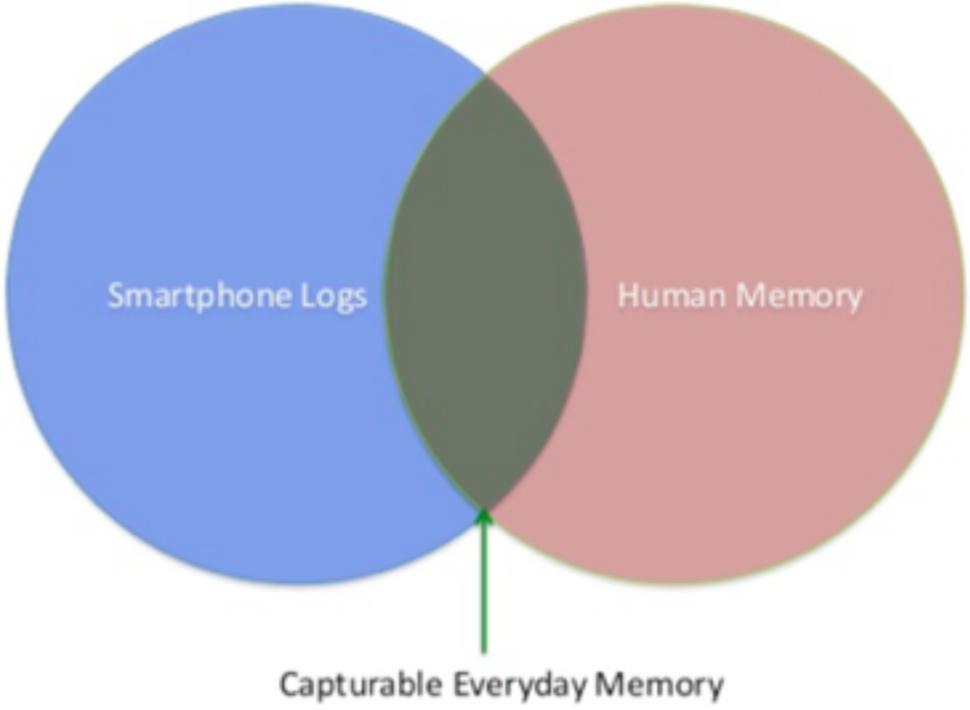
Sauvik Das
Carnegie Mellon University
sauvik@cmu.edu

Eiji Hayashi
Carnegie Mellon University
ehayashi@cs.cmu.edu

Jason Hong
Carnegie Mellon University
jasonh@cs.cmu.edu



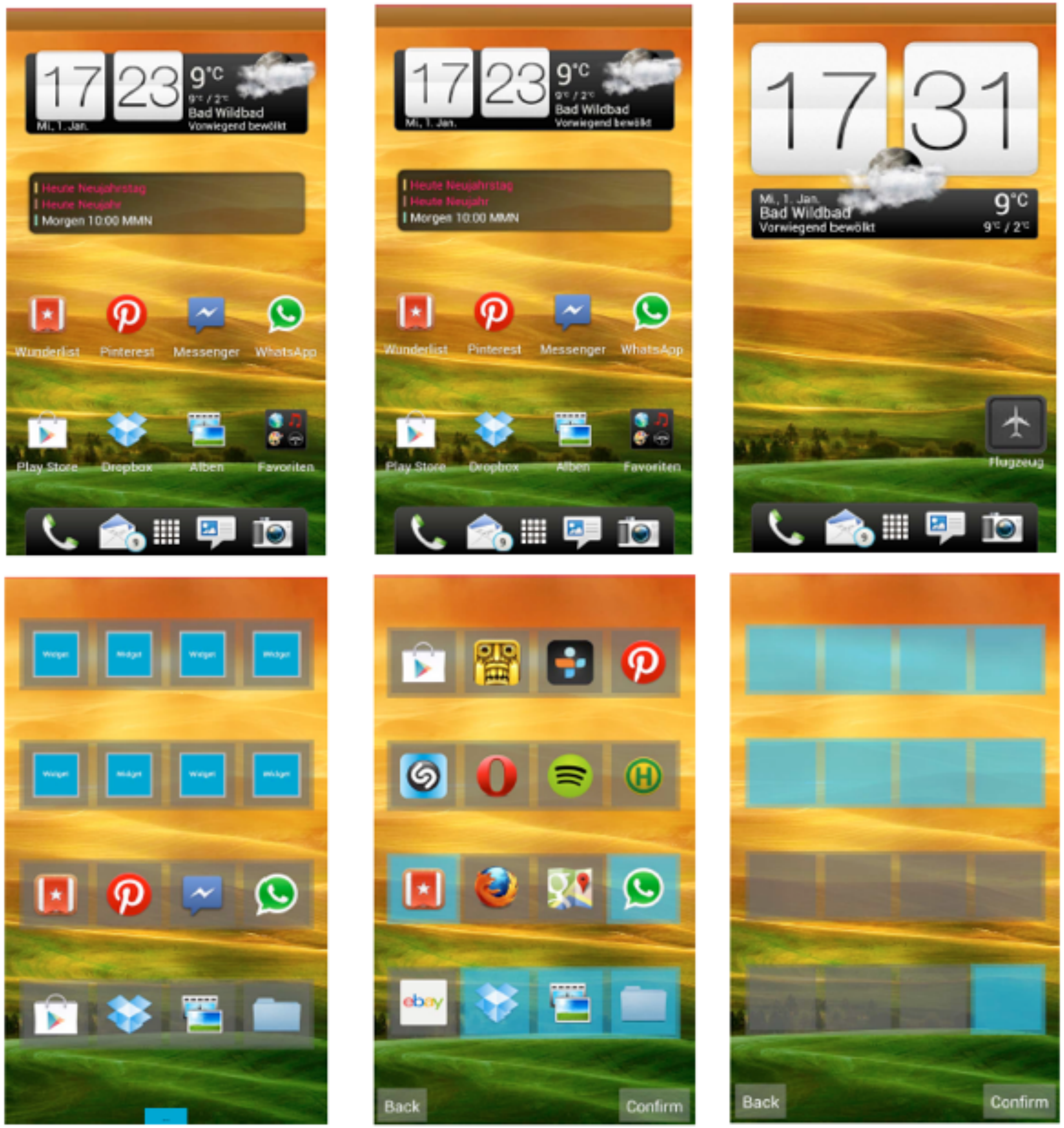
QType	Likert-scale prompts in Study 2.
FBApp	What application did you use on <time>?
FBLoc	Where were you on <time>?
FBOCall	Who did you call on <time>?
FBInCall	Who called you on <time>?
FBOSMS	Who did you SMS message on <time>?
FBInSMS	Who SMS messaged you on <time>?
FBIntSrc	What did you search the 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.



UBICOMP 2013
September 8-12
Zurich, Switzerland

http://sauvikdas.com/

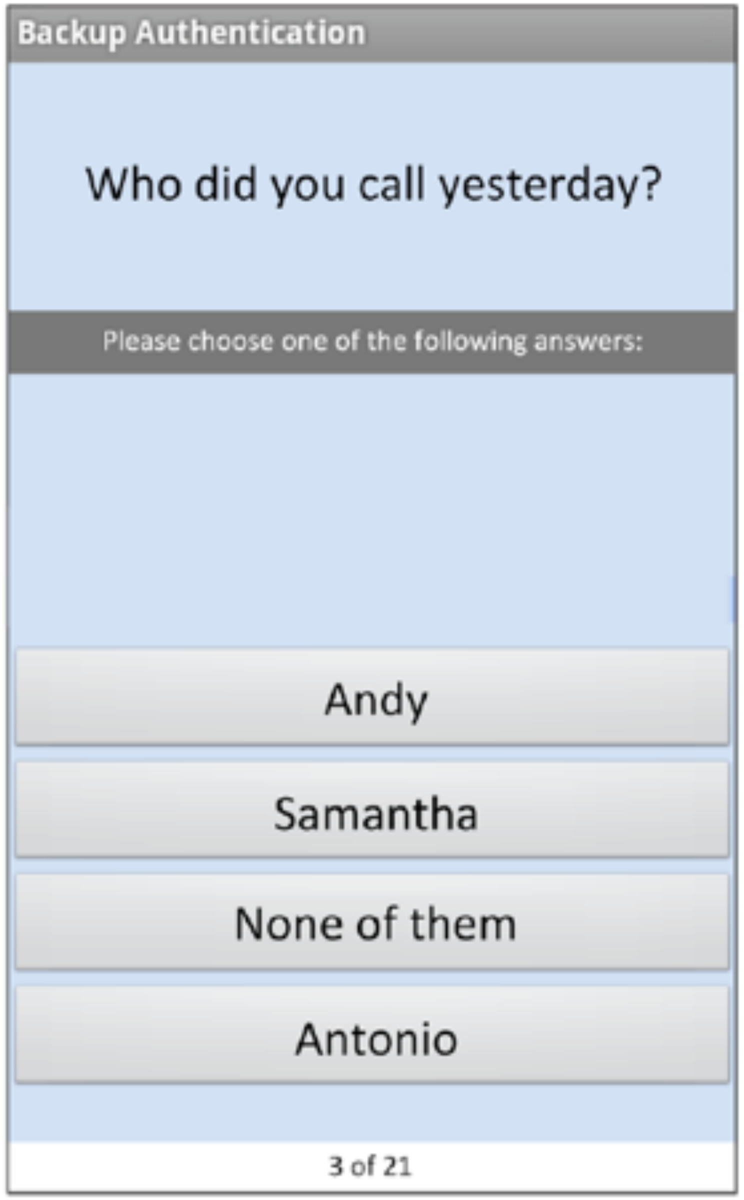
APP图标布局认证



Using Icon Arrangement for Fallback Authentication on Smartphones

Poster @ CHI 2014

动态安全问题



Backup Authentication

Who did you call yesterday?

Please choose one of the following answers:

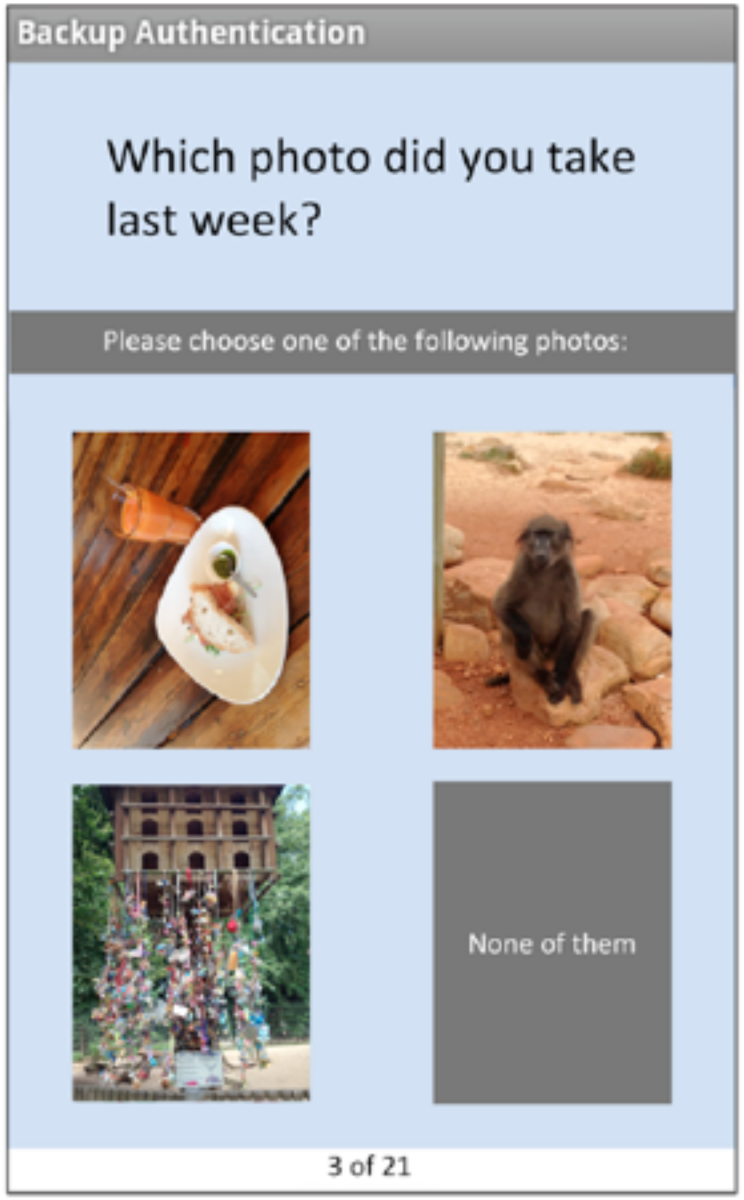
Andy

Samantha

None of them

Antonio

3 of 21



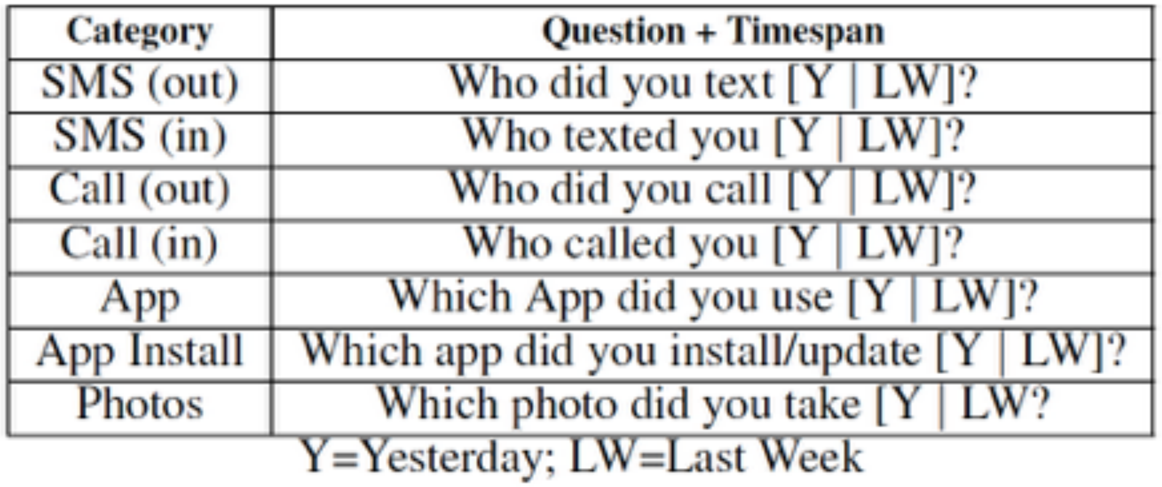
Backup Authentication

Which photo did you take last week?

Please choose one of the following photos:

None of them

3 of 21



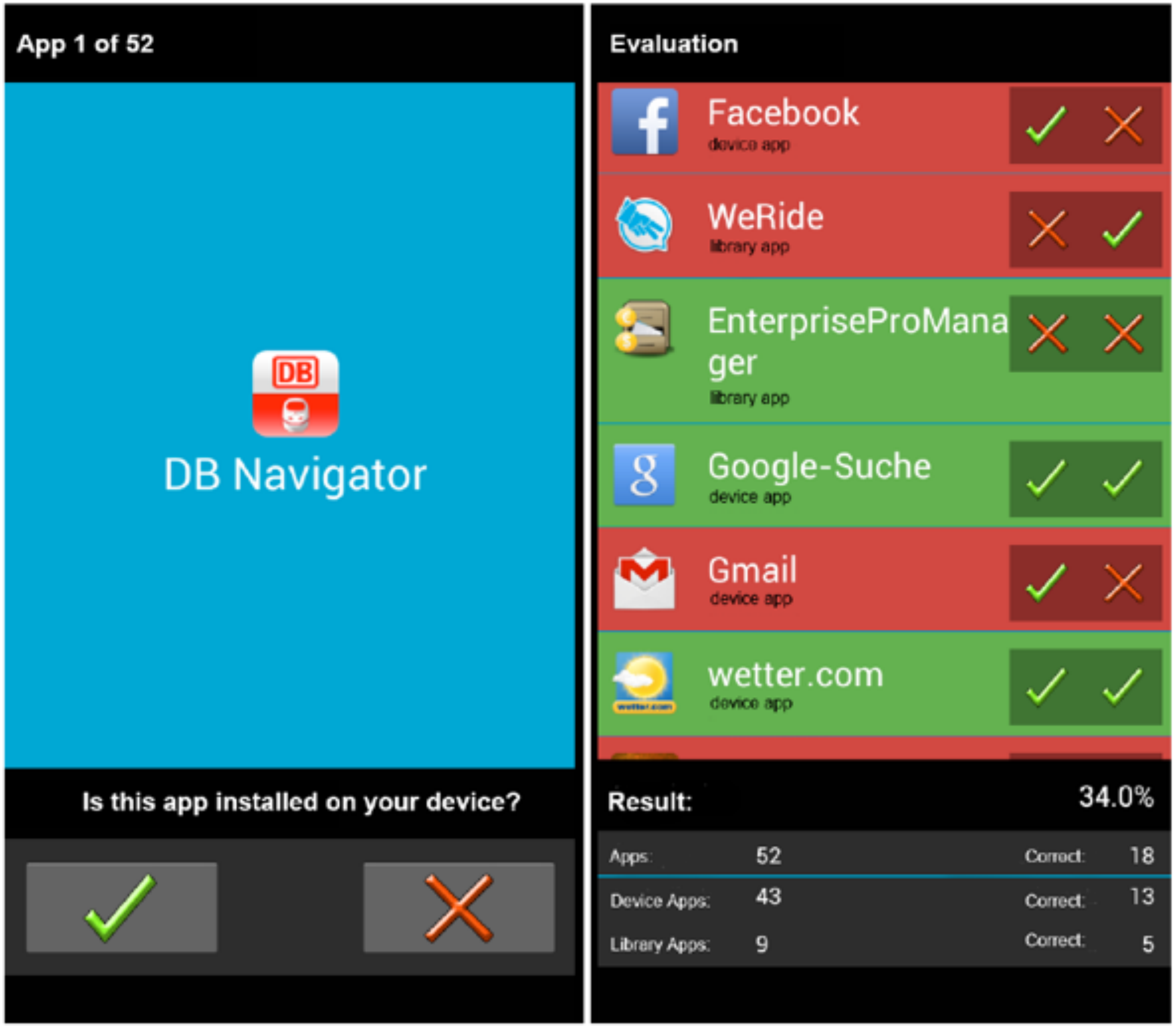
Category	Question + Timespan
SMS (out)	Who did you text [Y | LW]?
SMS (in)	Who texted you [Y | LW]?
Call (out)	Who did you call [Y | LW]?
Call (in)	Who called you [Y | LW]?
App	Which App did you use [Y | LW]?
App Install	Which app did you install/update [Y | LW]?
Photos	Which photo did you take [Y |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

动态安全问题 – APP安装



Is this app installed on your device?

Result: 34.0%

Apps:	52	Correct:	18
Device Apps:	43	Correct:	13
Library Apps:	9	Correct:	5

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

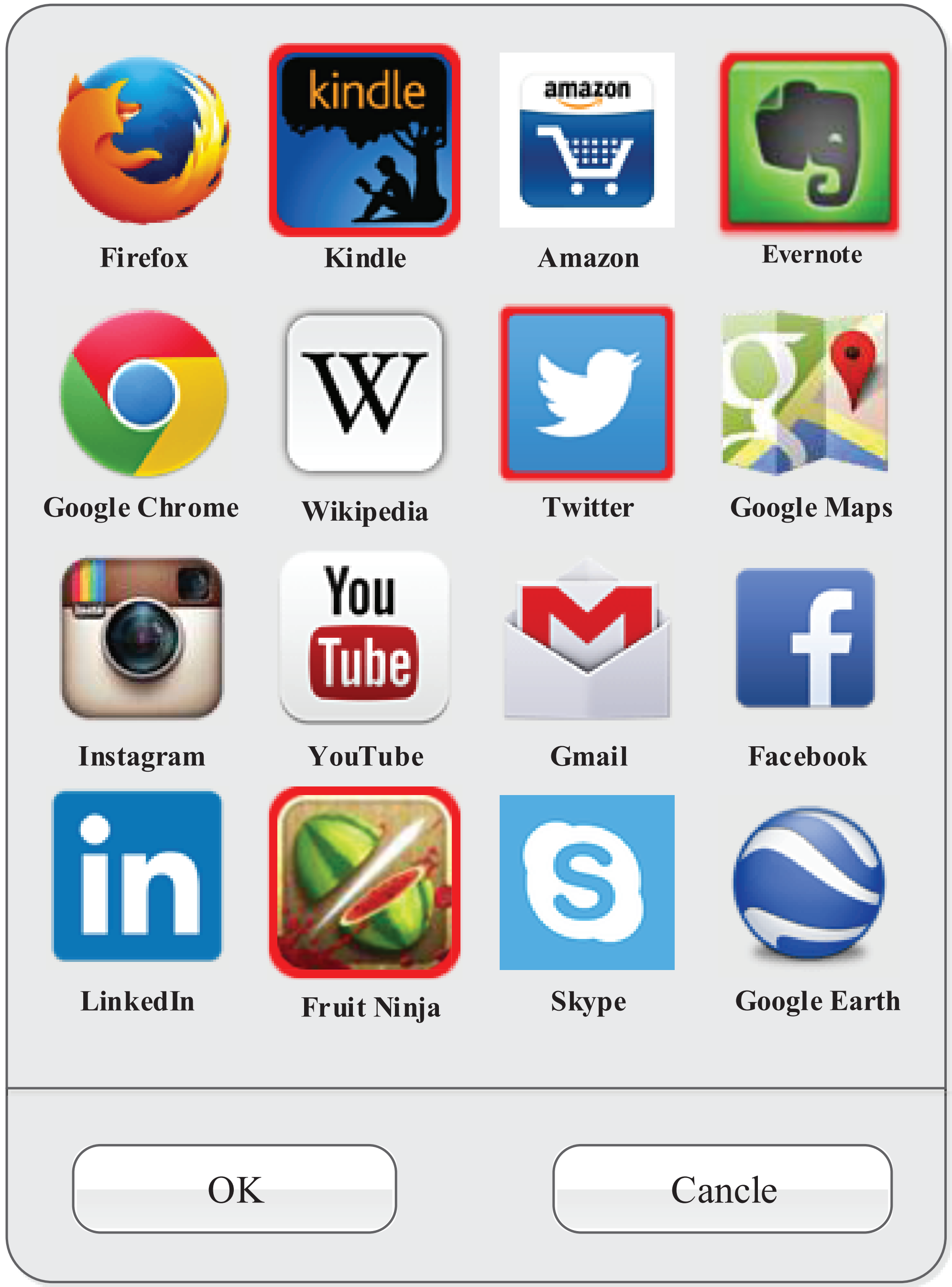
PassApp

is a novel recognition-based graphical password which utilises user's

installed apps

on their mobile devices

as password

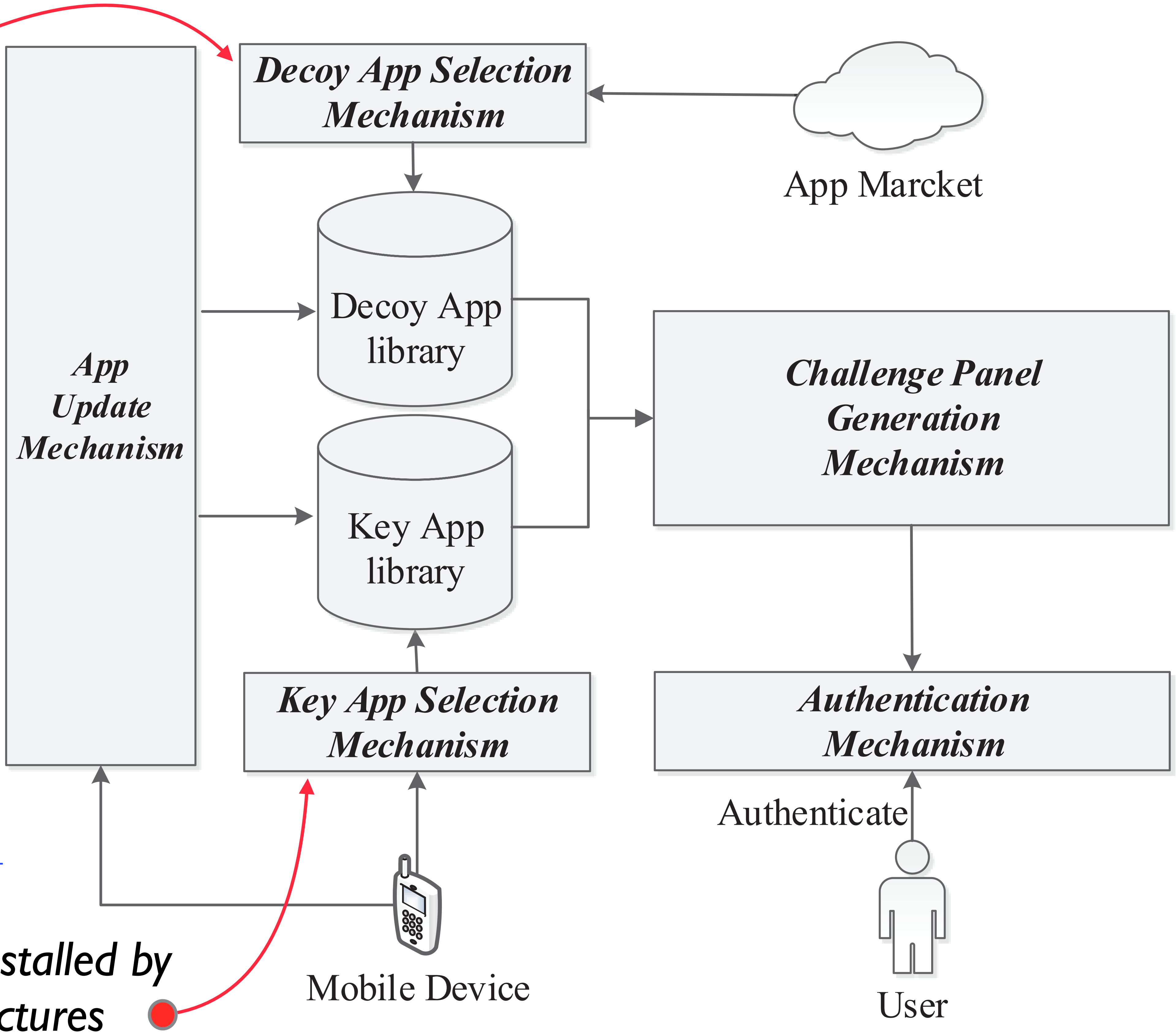


PassApp Mechanism

same category, similar ranks, etc

install a new app: add this app as key app, add 3 decoy apps

uninstall a app: delete this app from key app libs and move it into blacklist, remove corresponding decoy apps from decoy app libs

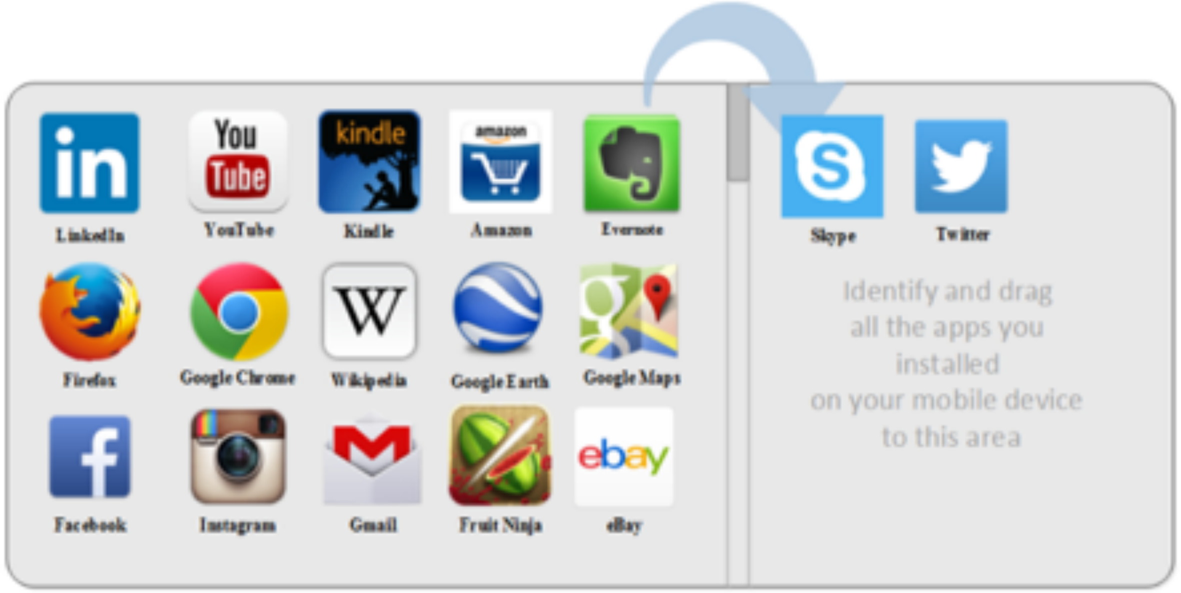


rule out the apps preinstalled by device and OS manufactures

User Study

Day 1

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

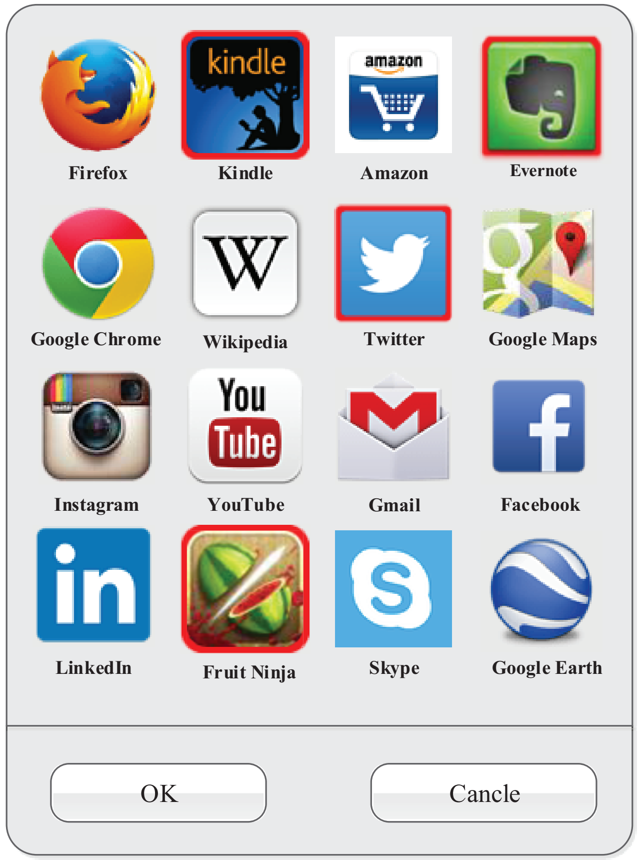


Identify and drag all the apps you installed on your mobile device to this area

42 participants

Day 2

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



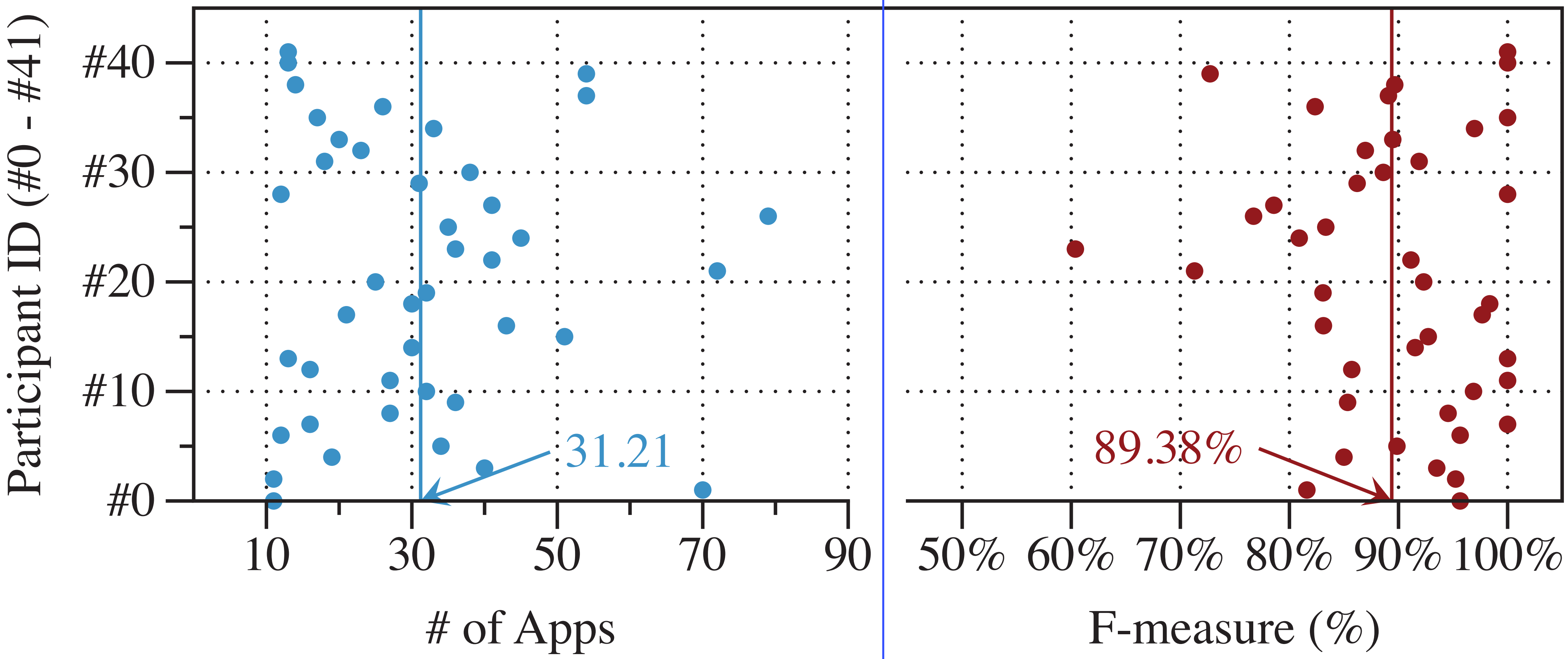
unlock10 times

42 *10

Login Time

Success Rate

Memory about Installed Apps



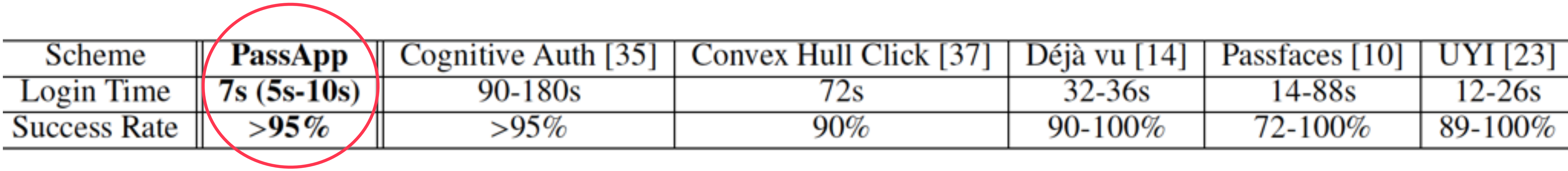
Max:79, Min: 11, SD: 16.79

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

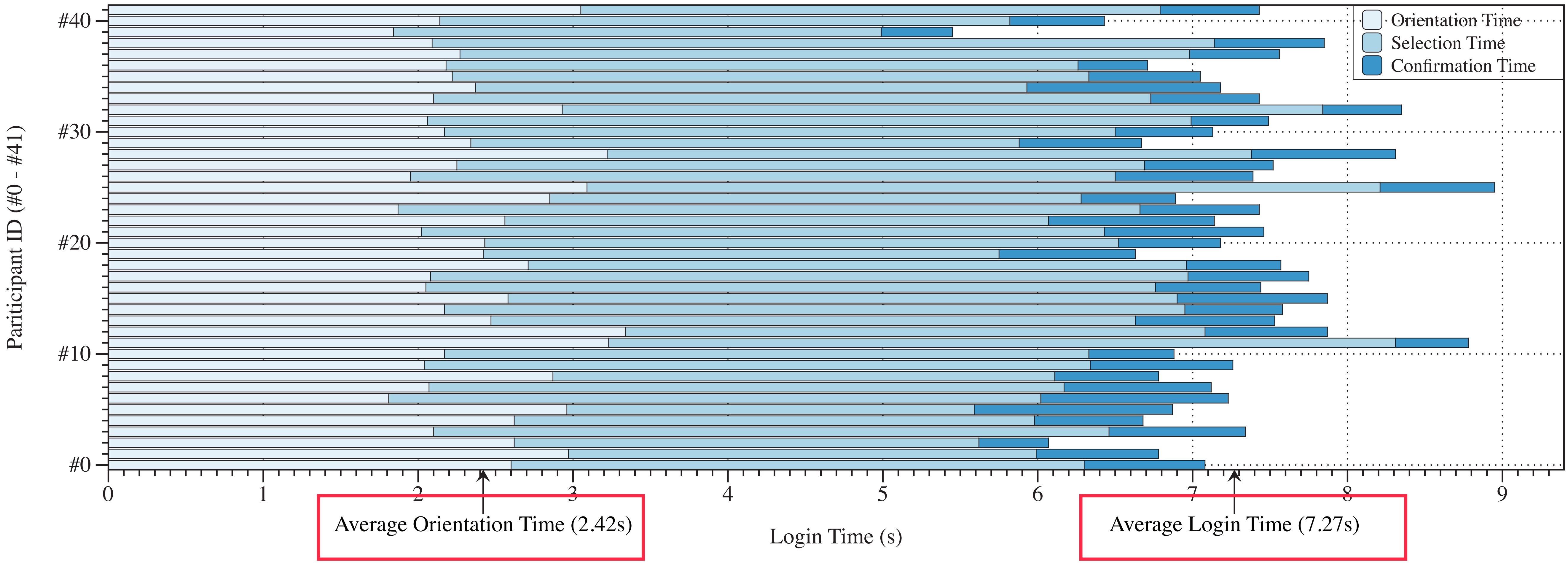
$$P(precision) = \frac{\sum picked\ installed\ apps}{\sum all\ apps\ picked}$$

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

Login Time and Success Rate



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

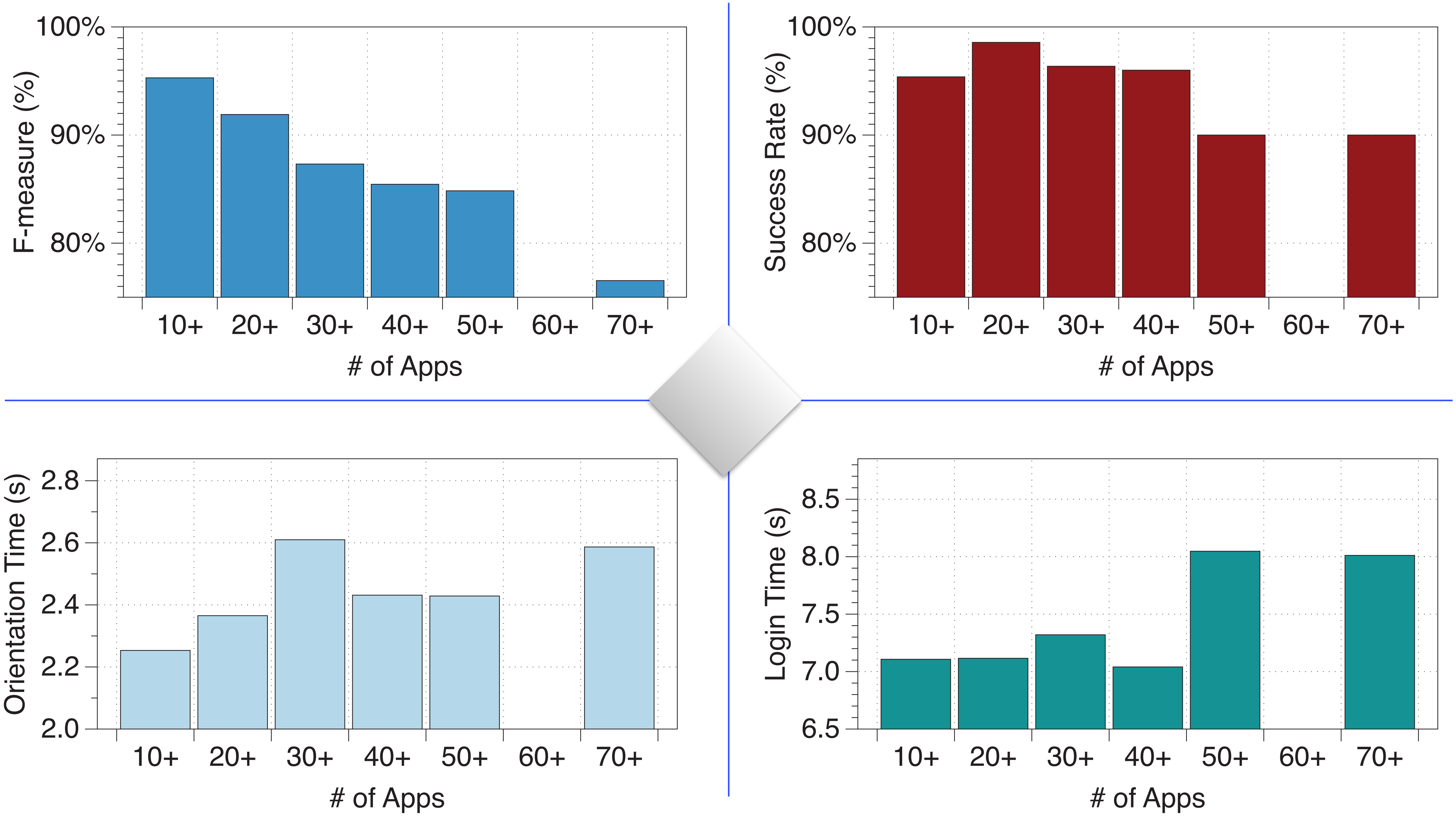


Average Orientation Time (2.42s)

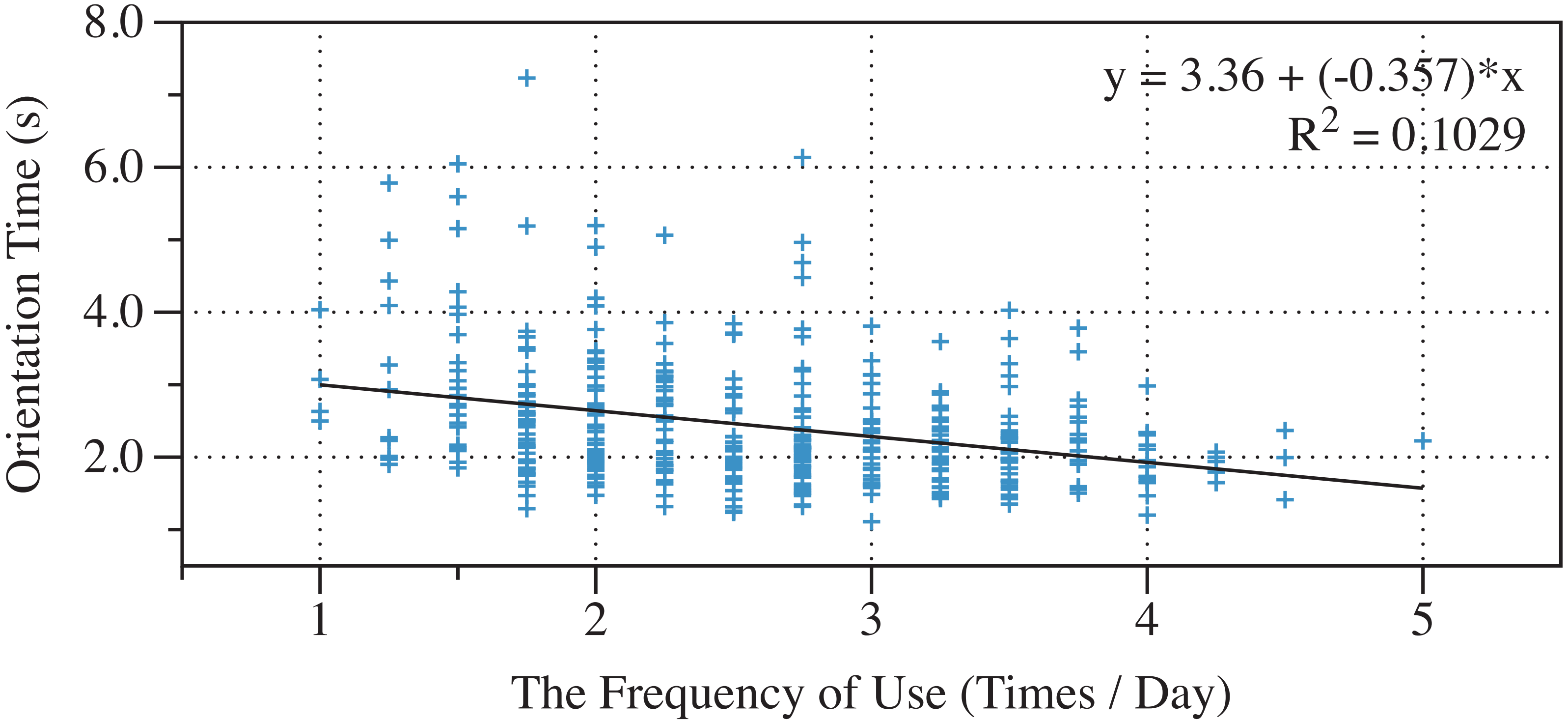
Average Login Time (7.27s)

Average confirmation time: 0.76s

Number of Key Apps & Usability Indices



Frequency of Using Apps & Usability Indices



28.38% <0.2times/days

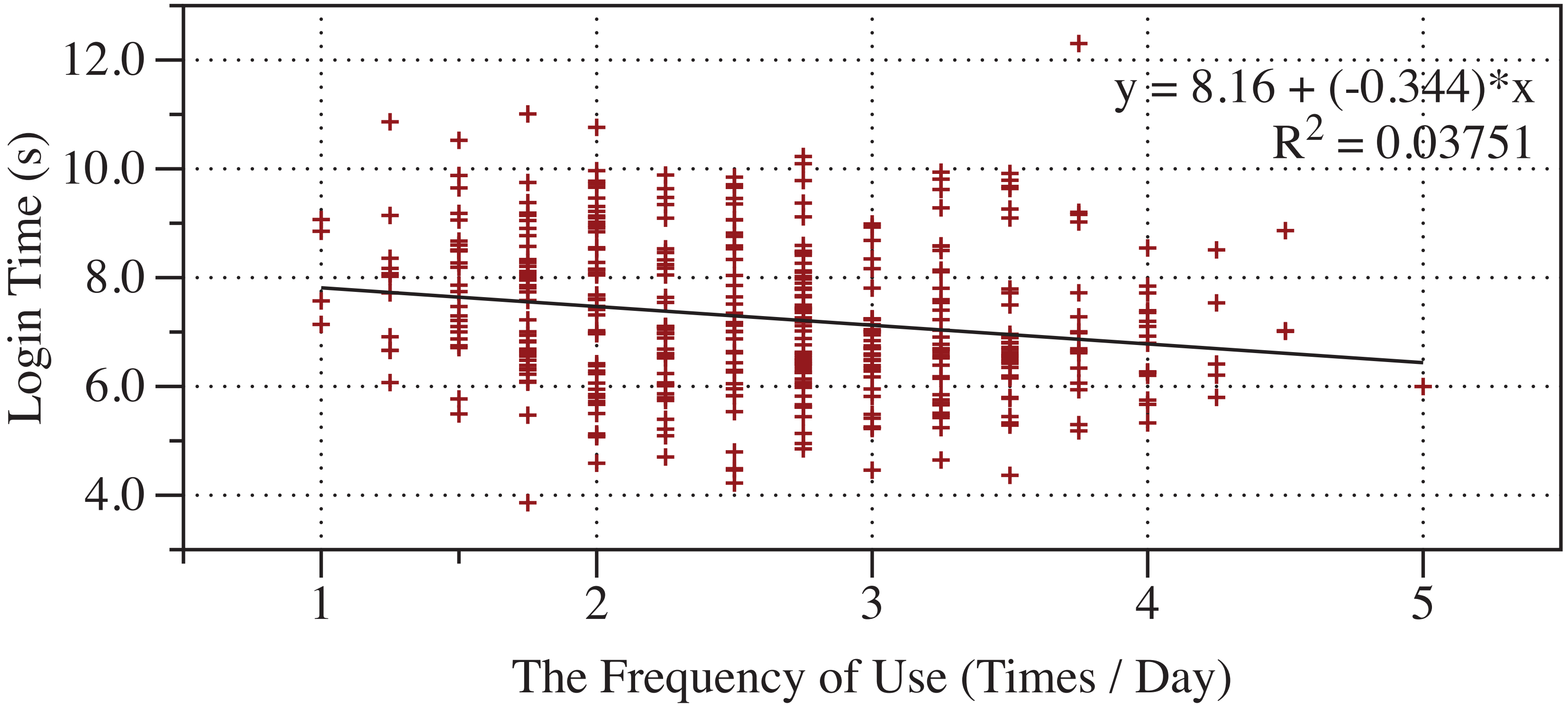
21.66% 0.2 -0.5 t/d

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

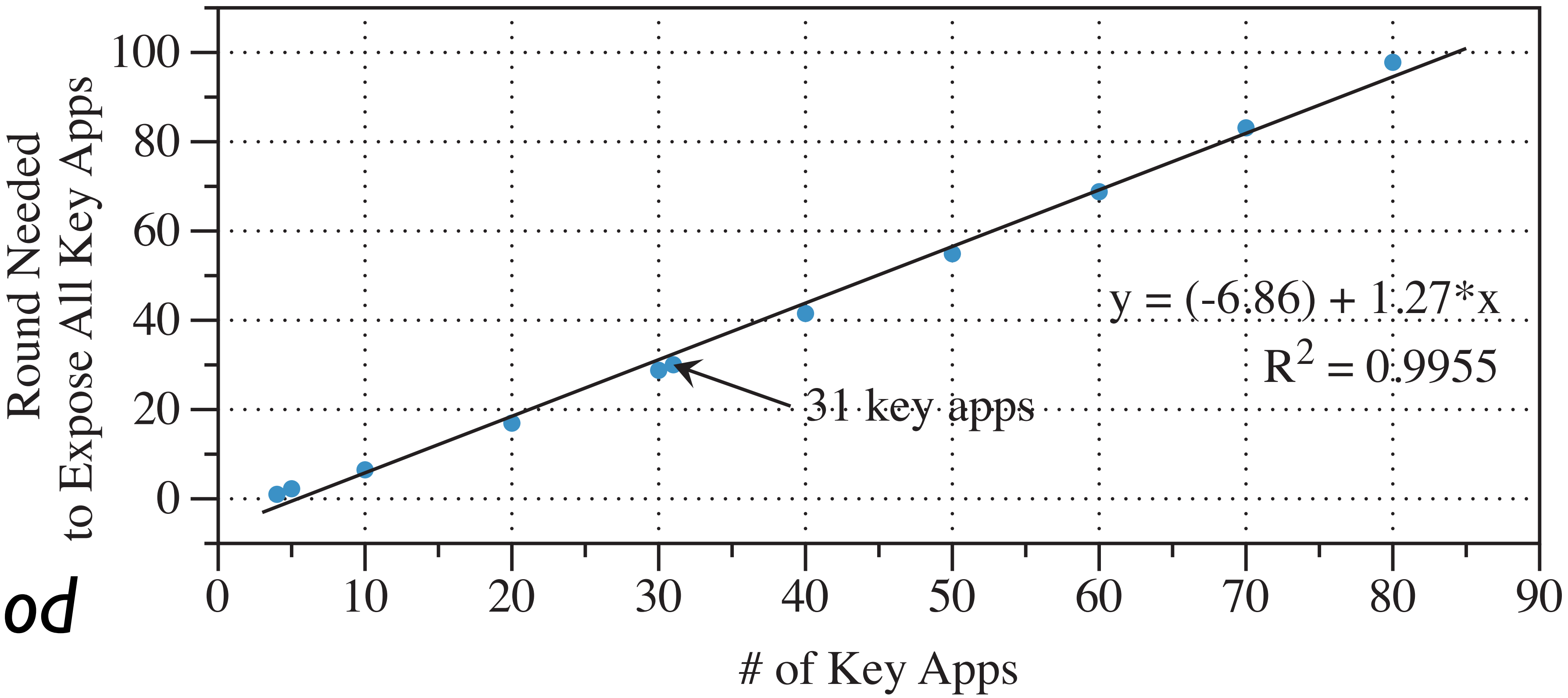
$$1/\binom{16}{4} = 1/1820.$$

0.055%

One-time shoulder Surfing Attacks

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

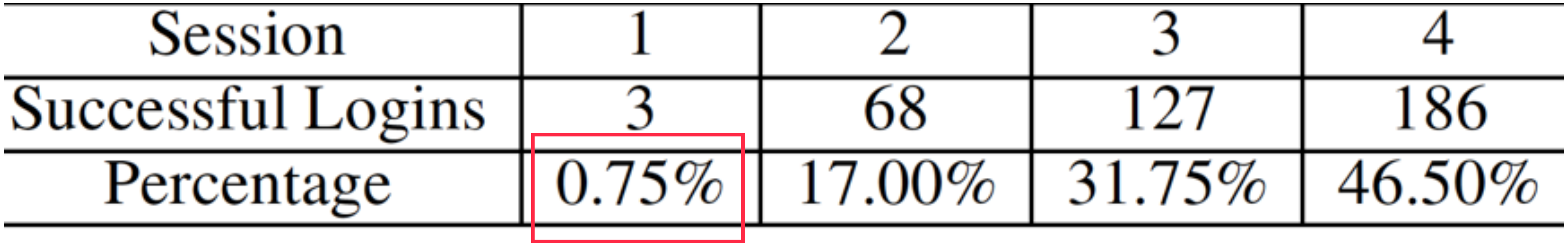
Multi-time shoulder Surfing Attacks



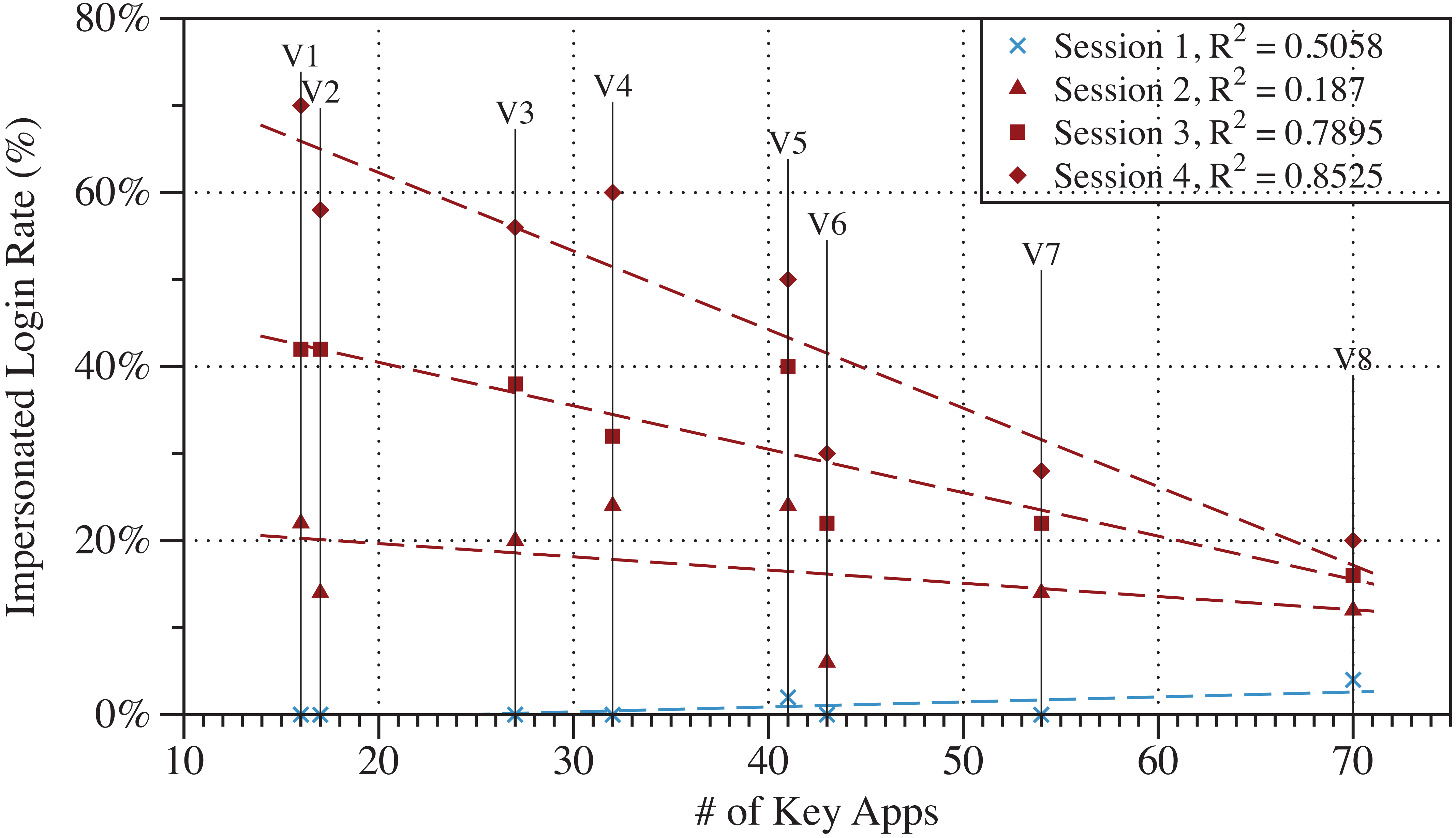
Monte Carlo Method

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)*

图形口令评价

可用性 vs. 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

任务

- **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

安全

- **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

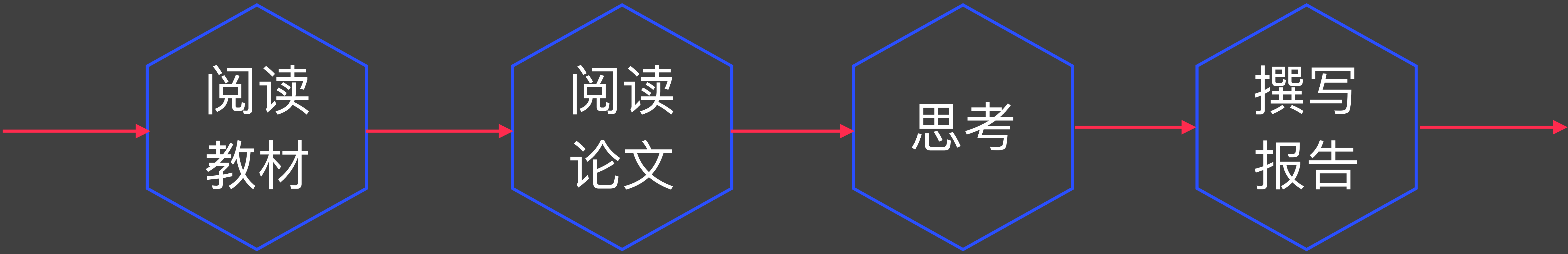
评估方法

- 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

提问时间！

课后作业



阅读教材

阅读论文

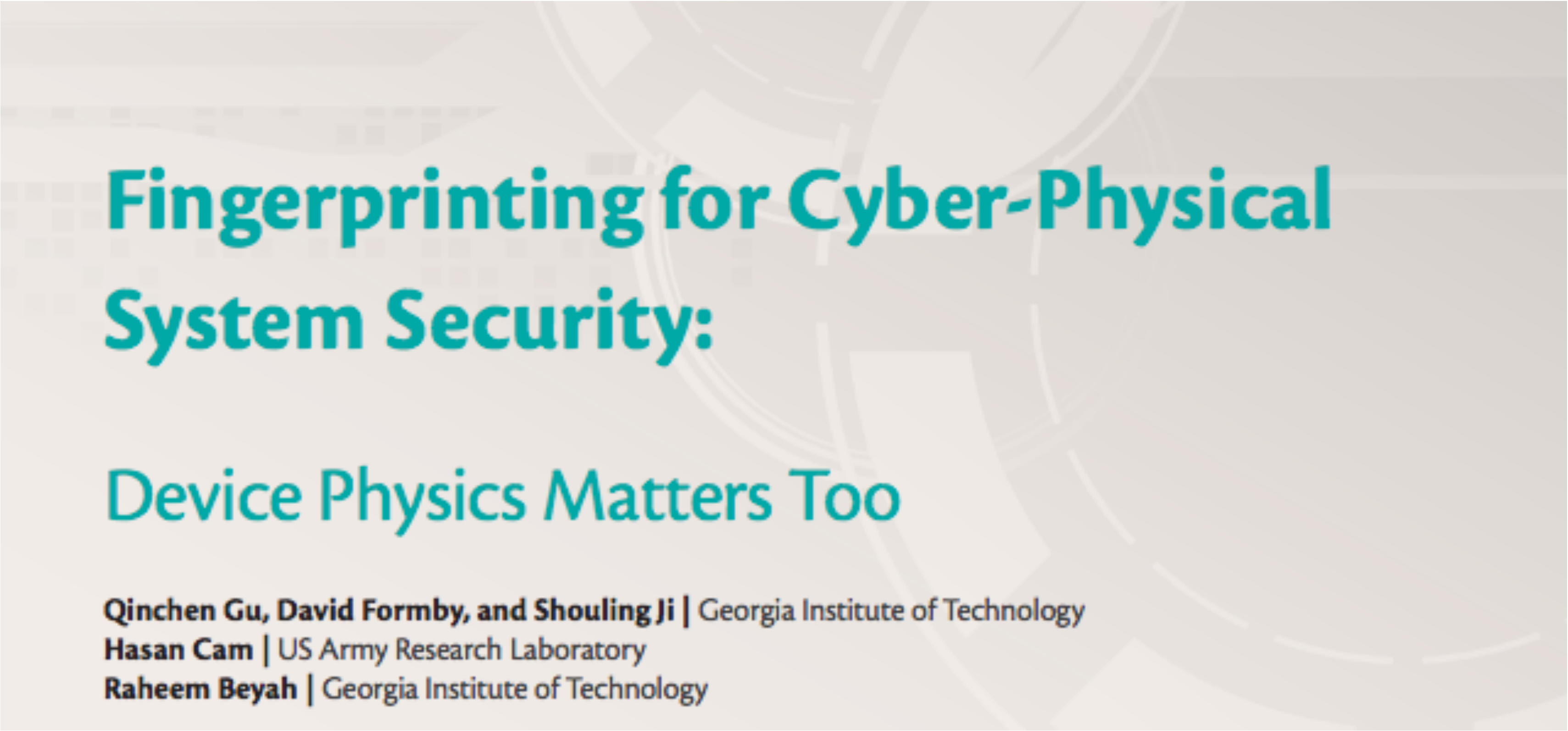
思考

撰写报告

Homework

课后作业

要求阅读如下文章，写阅读报告



Fingerprinting for Cyber-Physical System Security:

Device Physics Matters Too

Qinchen Gu, David Formby, and Shouling Ji | Georgia Institute of Technology
Hasan Cam | US Army Research Laboratory
Raheem Beyah | Georgia Institute of Technology

IEEE Security & Privacy Magazine 2018

检索一篇设备指纹相关的2017-2018的论文，简单阅读，杂志的文章最好

1、文章概述

2、主要收获

3、存在疑问

4、所思所感

5、一篇论文

周六晚上12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io