Information Security Engineering

2020.09.30

可用安全

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

上次课程内容回顾

1 课程简介

- 基本信息
- 课程内容
- 课程教材
- 课程组织
- 考核方式

2 信息安全经济学

- 安全
- 信息安全工程
- 柠檬市场
- 网络外部性
- 考虑安全

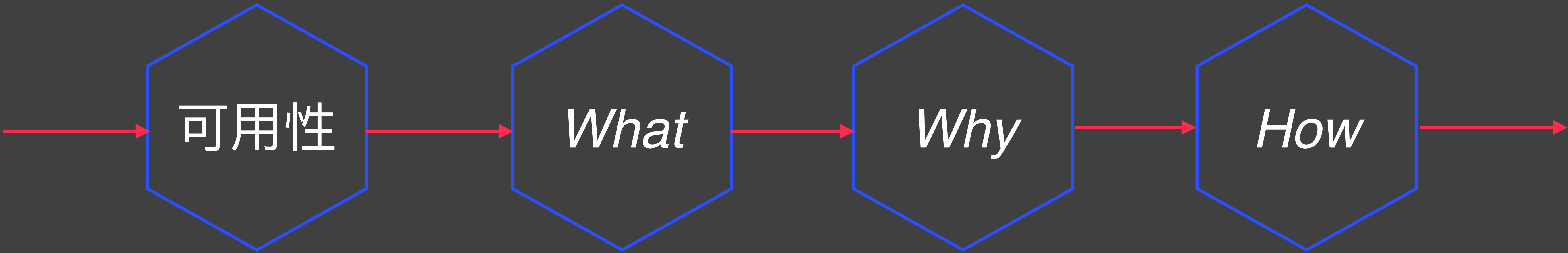
3 安全、信任、信用

- 社会工程学
- 可用安全
- 活体检测
- 信任信誉
- 信用评分

4 其余

- 图灵测试
- MTurk
- 设备指纹
- 分布式系统
- 区块链

可用安全概述



可用性

What

Why

How

可用性定义

- 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*

主观满意度 ★
是用户在使用产品过程中所感受到的主观满意和接受程度

有效性 ★
是用户完成特定任务和达成特定目标时所具有的正确和完整程度

效率 ★
是用户完成任务的正确和完成程度与所用资源（如时间）之间的比率

能用

易用

易学性 ★
产品是否易于学习

用户满意度★
用户对产品是否满意

易记性 ★
客户搁置一段时间后是否仍然记得如何操作

交互效率 ★
使用产品完成具体任务的效率

错误 ★
操作错误出现的频率和严重程度如何

Jakob Nielsen

https://www.nngroup.com/people/jakob-nielsen/

可用性评估

- 专家评估 / 用户实验 / 实际使用
- lab study / field study
- 问卷 / 访谈
- 实验人数、多个session、盲试
- IRB：伦理审查
- 专家 / 频繁使用 / 不频繁使用 / 特殊用户
- 设备和环境的不同
- 基于Web：Amazon Mechanical Turk

可用安全起源

- 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.

—The Protection of Information in Computer System. In Proc. IEEE 1975

- ***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*

计算机能力

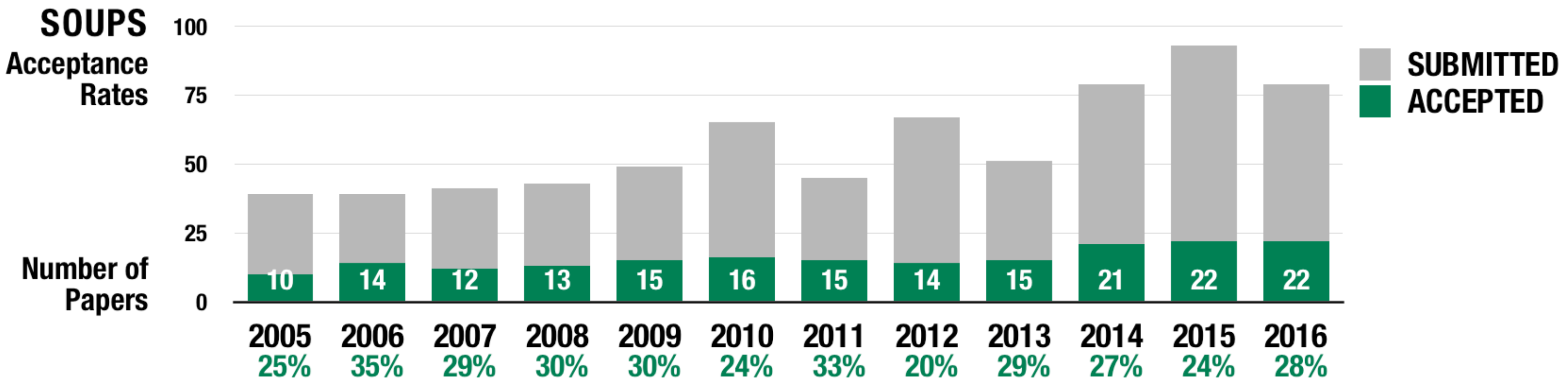
计算、存储、网络、普及、…

用户要求

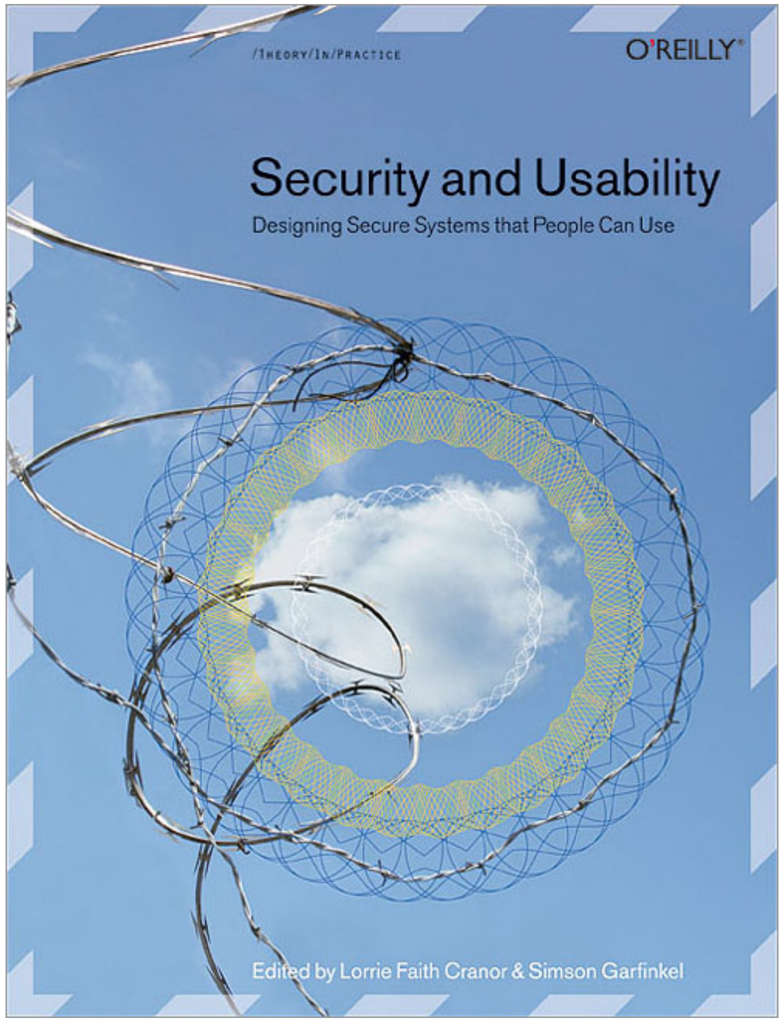
角色、需求、竞争、消失、…

SOUPS

Security and Usability： Designing Secure Systems that People Can Use (2005)



http://shop.oreilly.com/product/9780596008277.do


/THEORY/IN/PRACTICE
O'REILLY
Security and Usability
Designing Secure Systems that People Can Use
Edited by Lorrie Faith Cranor & Simson Garfinkel

http://cups.cs.cmu.edu/soups/

- Innovative security or privacy functionality and design
- Field studies of security or privacy technology
- Usability evaluations of new or existing security or privacy features
- Security testing of new or existing usability features
- Longitudinal studies of deployed security or privacy features
- Studies of administrators or developers and support for security and privacy
- The impact of organizational policy or procurement decisions
- Lessons learned from the deployment and use of usable privacy and security features
- Foundational principles of usable security or privacy
- Ethical, psychological, sociological aspects of usable security and privacy
- Usable security and privacy implications/solutions for specific domains (e.g., IoT, medical, vulnerable populations)
- Replicating or extending important previously published studies and experiments
- Systematization of knowledge papers that integrate and systematize existing knowledge to provide new insight into a previously studied area

https://www.usenix.org/conference/soups2020/call-for-papers

Symposium on Usable Privacy and Security (2005-Present)

可用安全

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，安全技术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（人机交互）与信息安全
- 超越UI：改变用户和开发者习惯和思路

HCISec

为什么需要可用安全

- 开发人员和用户对安全和可用的认识是不同的
- 不同的用户的认识也是不同的

- 安全增加了障碍：If you want security, you must be prepared for inconvenience
- 安全与可用不可调和

- **不可用的安全是容易的，可用的安全是非常困难的**

- 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
- 用户什么都不知道….

- 教育训练
- 设计时就需要考虑可用性
- 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

Usable Security Overview

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
- 安全和隐私可理解
- 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

自动化处理

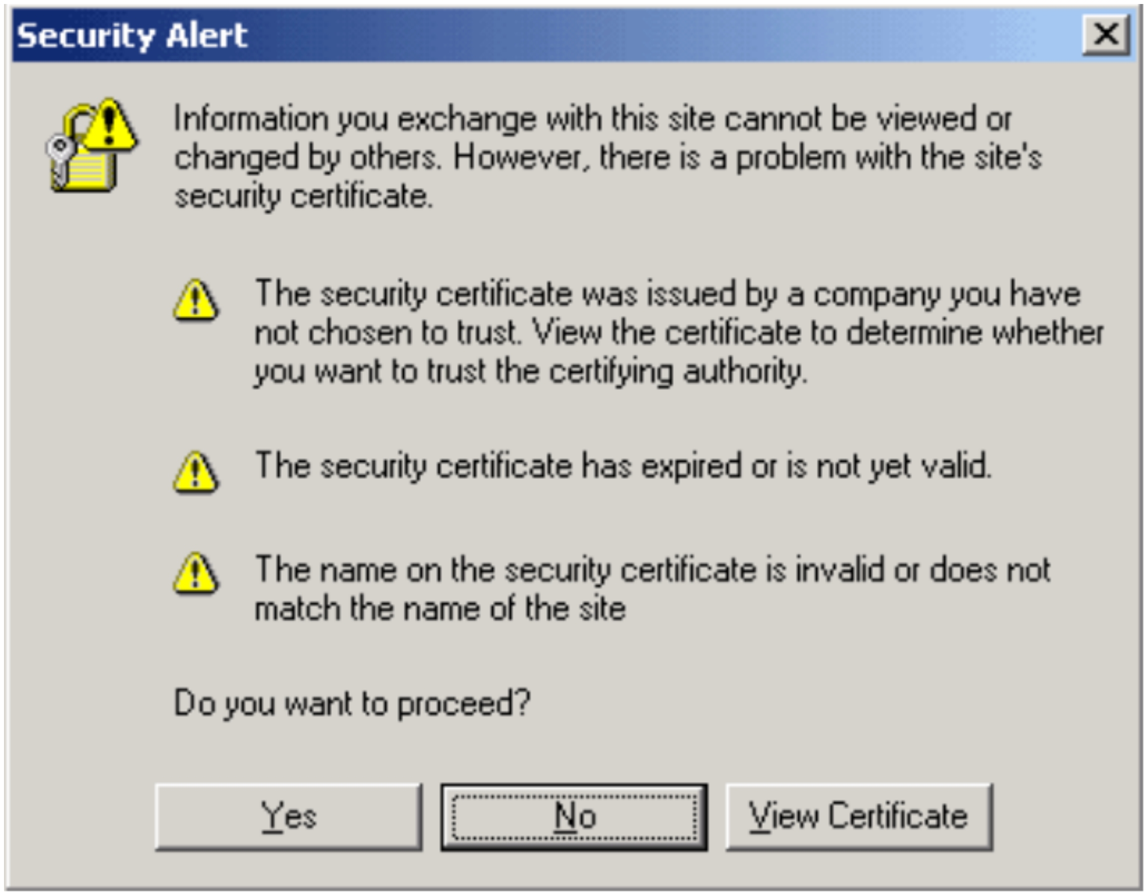
减少人机交互

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

安全问题

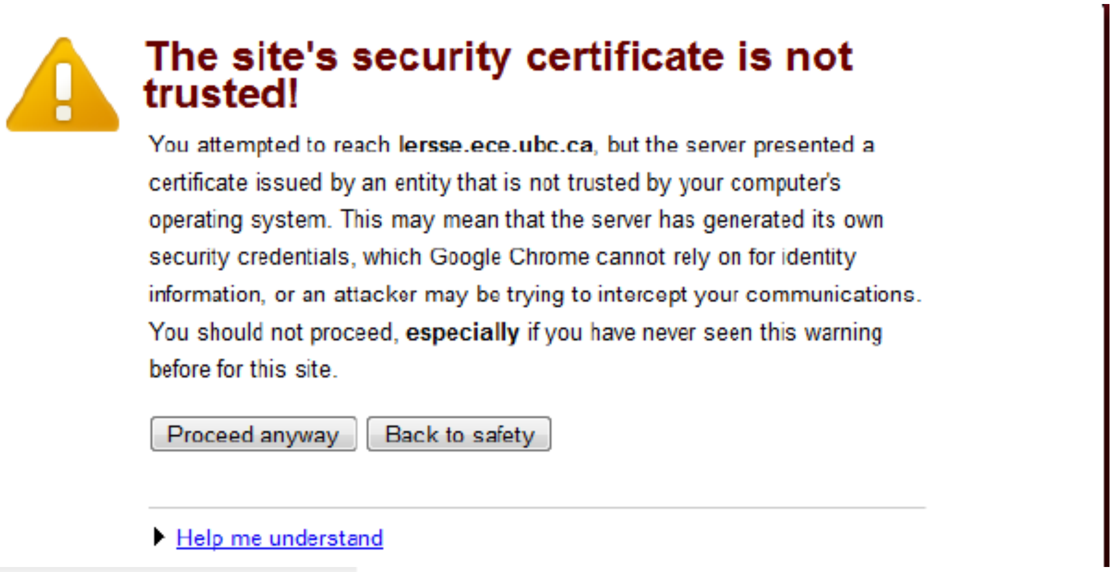


Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

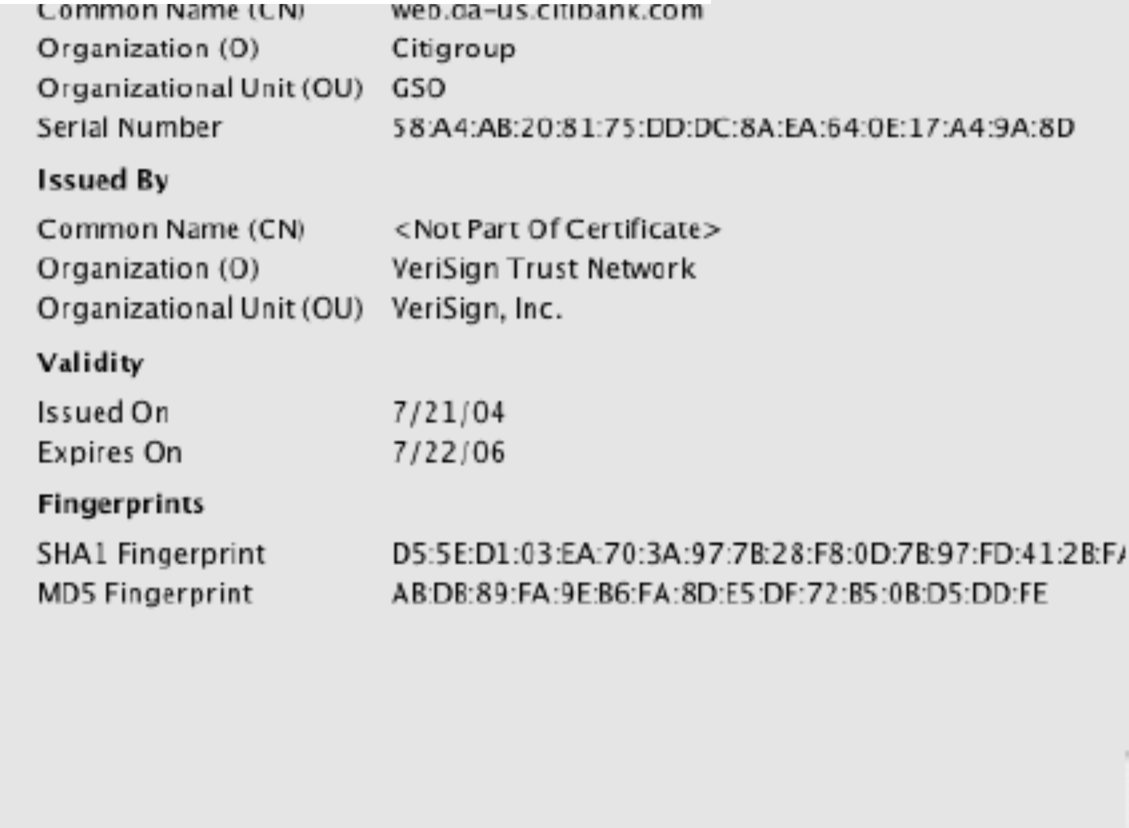
- The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- The security certificate has expired or is not yet valid.
- The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

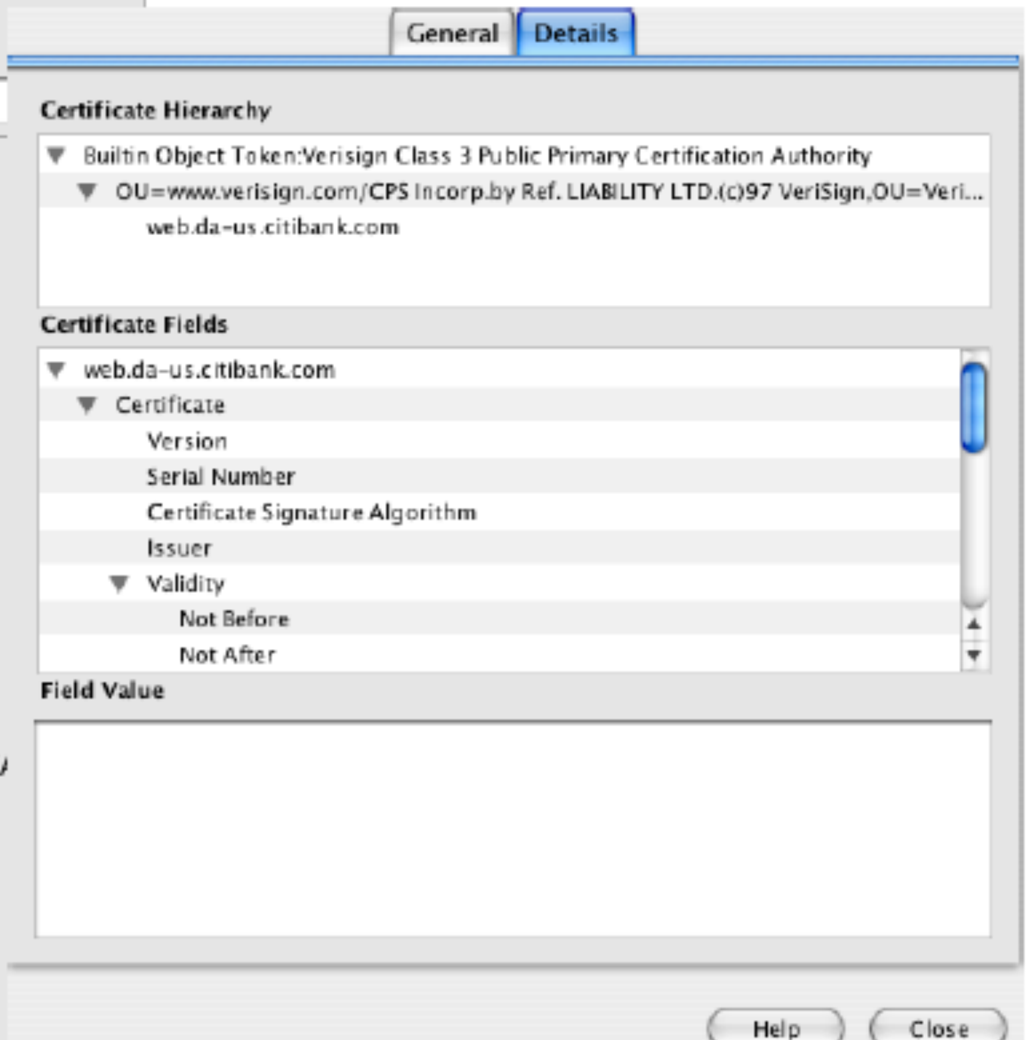


The site's security certificate is not trusted!

You attempted to reach **lersse.ece.ubc.ca**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.



Common Name (CN)	web.da-us.citibank.com
Organization (O)	Citigroup
Organizational Unit (OU)	GSO
Serial Number	58:A4:AB:20:81:75:DD:DC:8A:EA:64:0E:17:A4:9A:8D
Issued By	
Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.
Validity	
Issued On	7/21/04
Expires On	7/22/06
Fingerprints	
SHA1 Fingerprint	D5:5E:D1:03:EA:70:3A:97:7B:28:F8:0D:7B:97:FD:41:2B:F
MD5 Fingerprint	AB:DB:89:FA:9E:B6:FA:8D:E5:DF:72:B5:0B:D5:DD:FE



Certificate Hierarchy

- Builtin Object Token:Verisign Class 3 Public Primary Certification Authority
  - OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign,OU=Veri...
    - web.da-us.citibank.com

Certificate Fields

- web.da-us.citibank.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before
      - Not After

Field Value

Say OK to Any Question About Security

Privacy Bird

- Web站点隐私策略

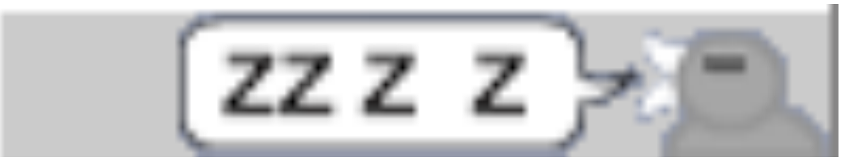
✶很多，但用户很少读

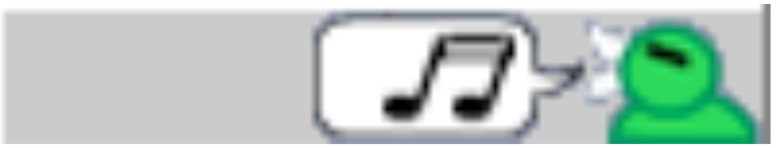
- Privacy Bird

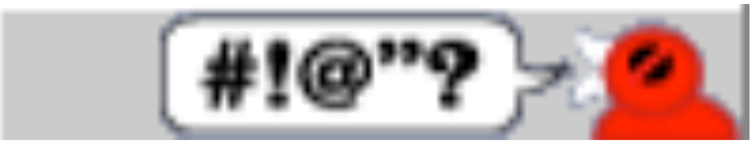
✶决定是否站点策略和用户隐私策略项匹配

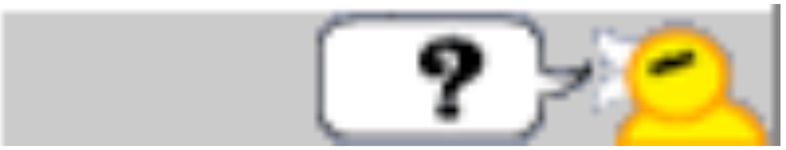
✶通知用户

http://www.privacybird.org/









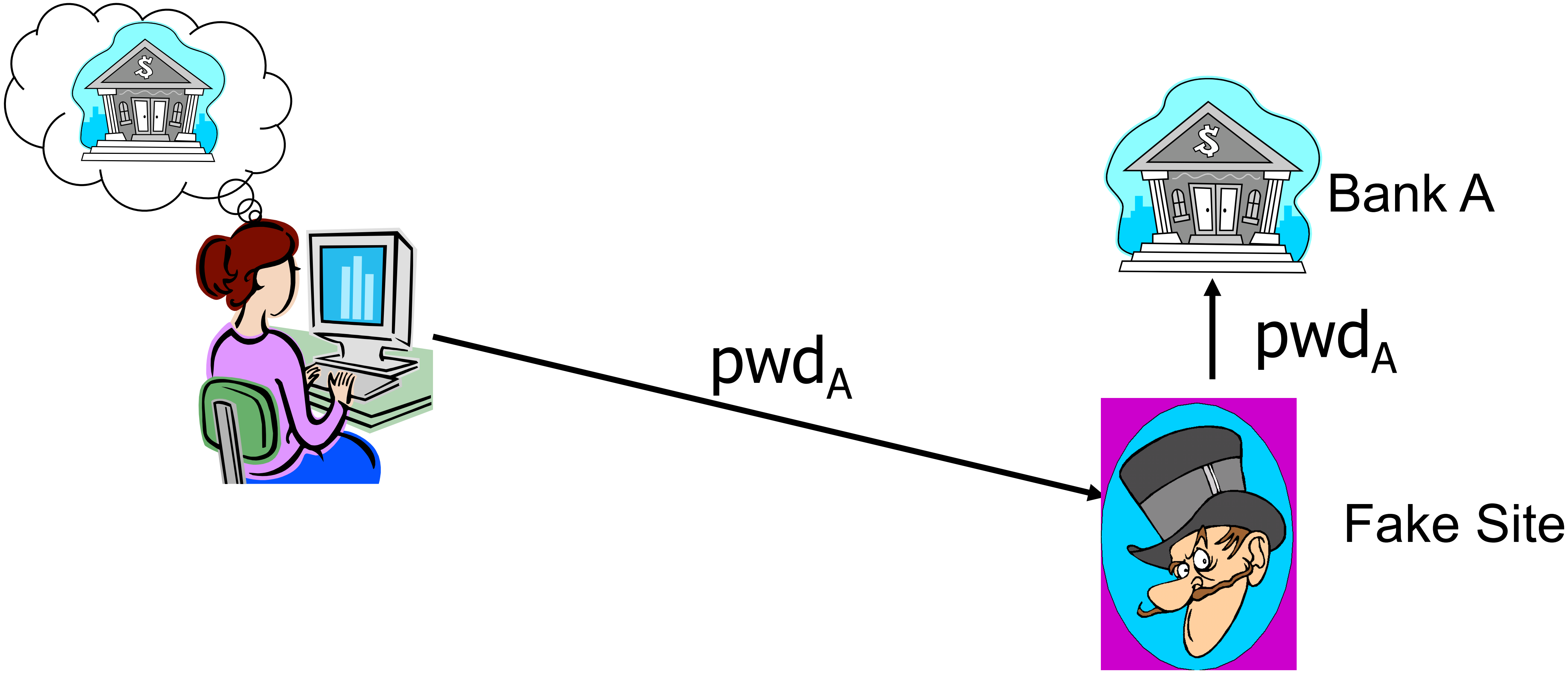
人的能力是有限的！

人是会犯错误的！

人与人是不同的！

网络钓鱼

- 对银行的网络钓鱼开始于2003年
- 2006年，美国银行损失2亿美元



pwd_A

Bank A

pwd_A

Fake Site

文本口令

文本口令依然是最常用的认证机制

文本口令

- 文本口令是研究与使用最为广泛的身份认证方法，最常用的形式：用户名＋口令
- 选择原则：易于记忆，难于猜中或者发现，抗分析能力强

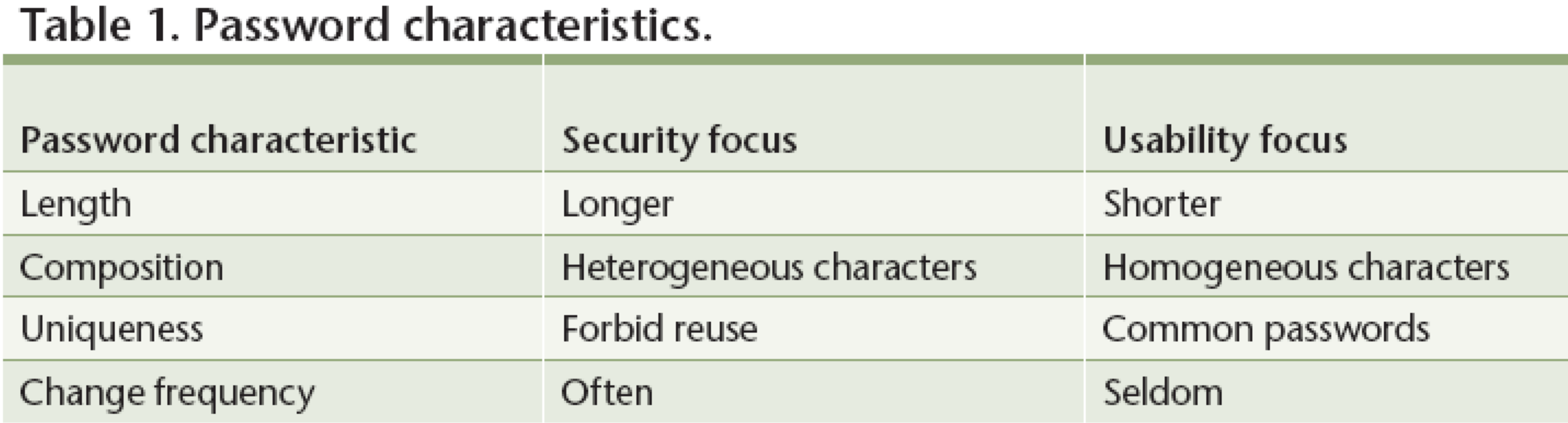


Table 1. Password characteristics.

Password characteristic	Security focus	Usability focus
Length	Longer	Shorter
Composition	Heterogeneous characters	Homogeneous characters
Uniqueness	Forbid reuse	Common passwords
Change frequency	Often	Seldom

Text Password

文本口令

- 为了证实标识或者获得存取资源的许可而用于身份认证的一个秘密的字或者一串字符

56年

1960

MIT CTSS

https://www.wired.com/2012/01/computer-password/

- *passphrase*、*passcode*、*personal identification number*、*watchword*、*access word*

Text Password

文本口令

Passwords Are Like Underwear
Passwords are like underwear... Change yours often.
Passwords are like underwear... Don't share them with friends.
Passwords are like underwear... The longer, the better.
Passwords are like underwear... Be mysterious.
Passwords are like underwear... Don't leave yours lying around.

I forgot the password for the file where I keep all my passwords.
www.maxine.com
JWagner
11-14

©2001 Hallmark Licensing, Inc./Dist. by Universal Press Syndicate

文本口令优缺点

- 容易使用
- 价格便宜
- 用户熟悉
- 隐私保护
- 携带方便

- 记忆困难
- 容易预测
- 多个账户
- 再次使用
- 可用影响

强口令

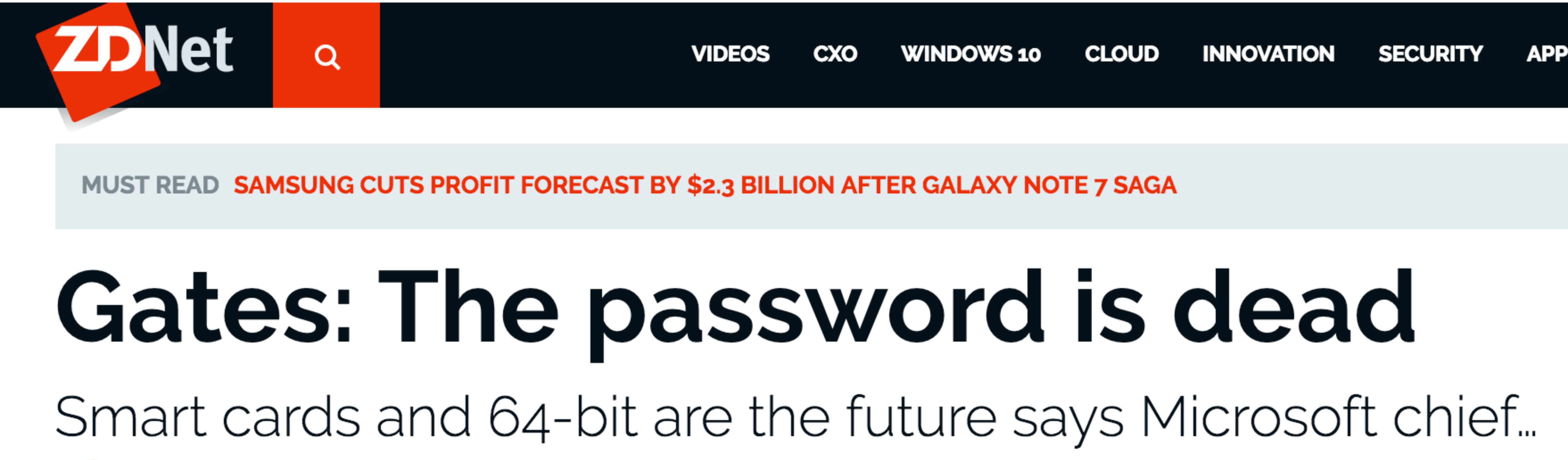
- 密码要足够长（至少7个字符）
- 包括大小写字母、数字和符号
- 六位必须至少有一个符号字符
- 至少使用四个不同的字符（不要重复同一字符）
- 使用随机数和字母
- 不要使用全部或部分登录名
- 不要使用任何语言中的实际词
- 不要使用数字代替类似的字母来构成单词
- 不要使用连续字母或数字（如“abcdefg”或“234567”）
- 不要使用键盘中的邻近键（如“qwerty”）

Password
is
Dead?

历史

- *1960: MIT CTSS*
- *1970: MULTICS，Hash存储*
- *1979: crypt()，hash＋salting*
- *1985: Green Book*
- *1985: NIST FIPS 112*

- *2004: Bill Gates, “the password is dead”*



MUST READ SAMSUNG CUTS PROFIT FORECAST BY $2.3 BILLION AFTER GALAXY NOTE 7 SAGA

Gates: The password is dead

Smart cards and 64-bit are the future says Microsoft chief...

攻击指纹

Chaos Computer Club

Theory

on Password has lagged

practice

口令建议和要求

- "Since many user-created password are particularly easy to guess, all passwords should be machine-generated"
- Users "shall be instructed to use a password selected at random, if possible, or to select one that is not related to their personal identity, history, or environment"
- "Pick something you cannot remember, and do not write it down"
- Independence when choosing multiple passwords
- … …

Users are also typically the most difficult component to model

Impossible for human to follow

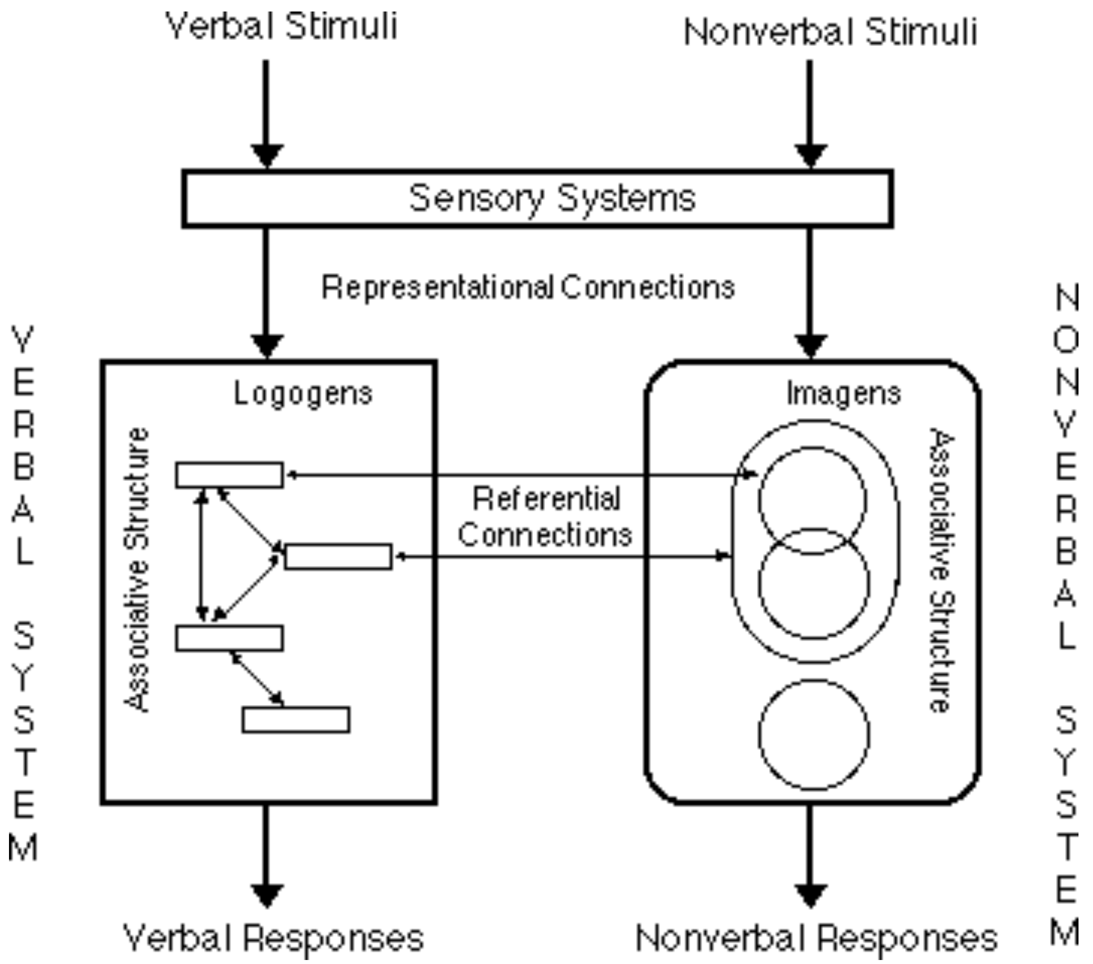
口令强度

- 口令的理论空间 *vs* 口令的实际空间
- 长度、构成元素、重复、相关性
- 安全性 *vs* 可用性
- 竞争性 *vs* 非竞争性
- 口令*checker vs blacklists*
- *offline vs online attack*
- 口令泄漏
- 三次失败锁定
- 提高强度的代价和收益

图形口令

使用图形作为口令构成元素

心理学基础



Dual Coding Theory

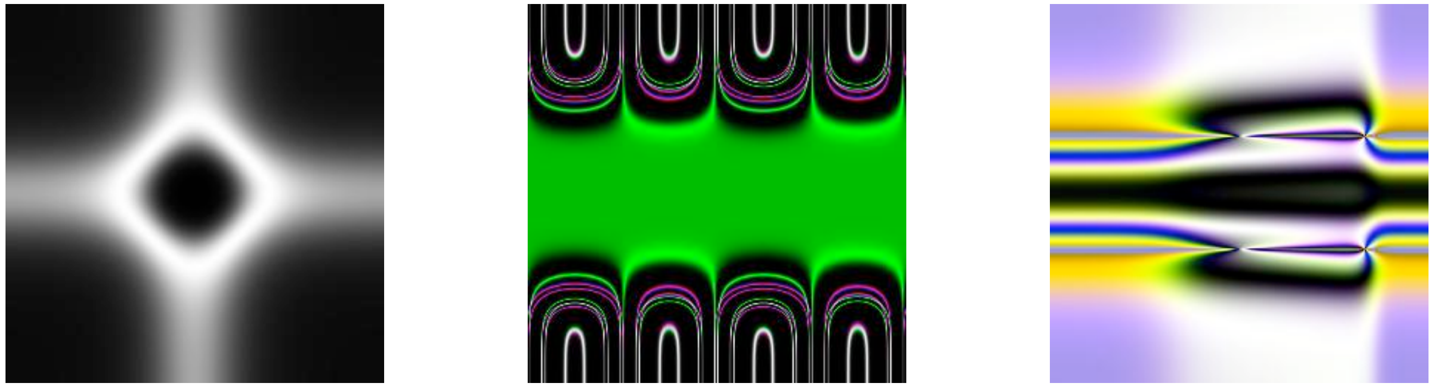
- Recall
- Recognition
- Cued Recall

Recognition is an easier memory task than recall

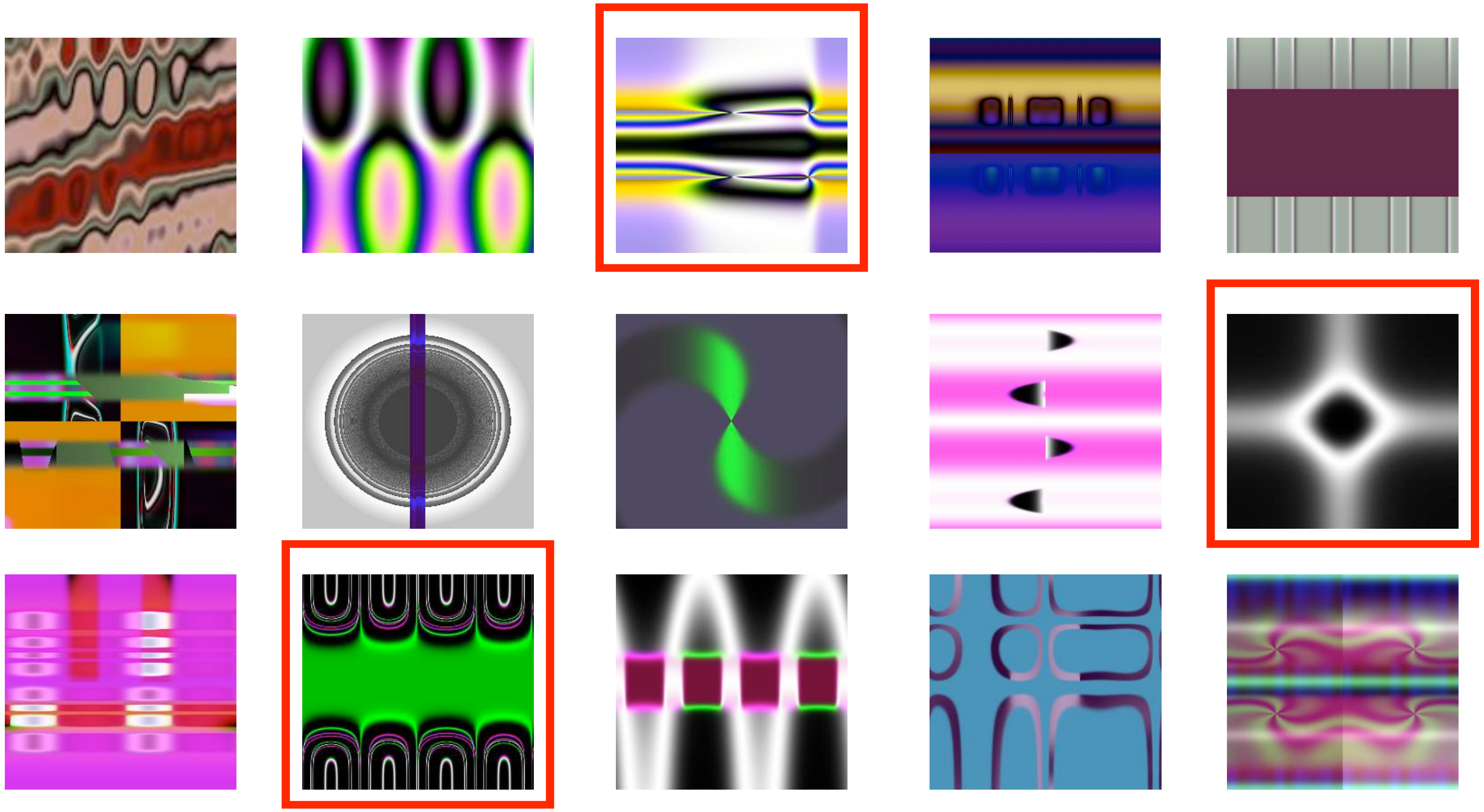
With the aid of a retrieval cue, more information can be retrieved

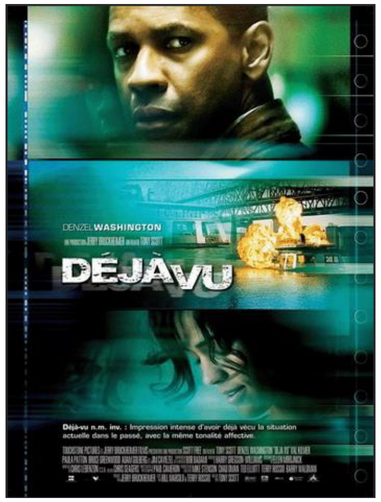
Déjà Vu

训练



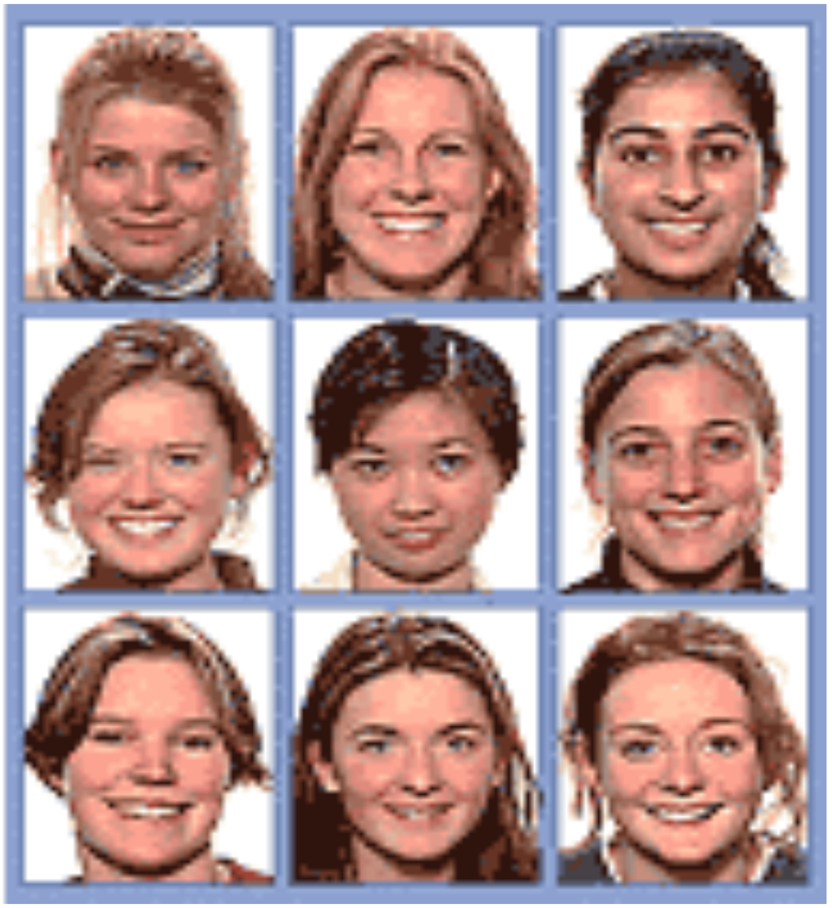
挑战





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

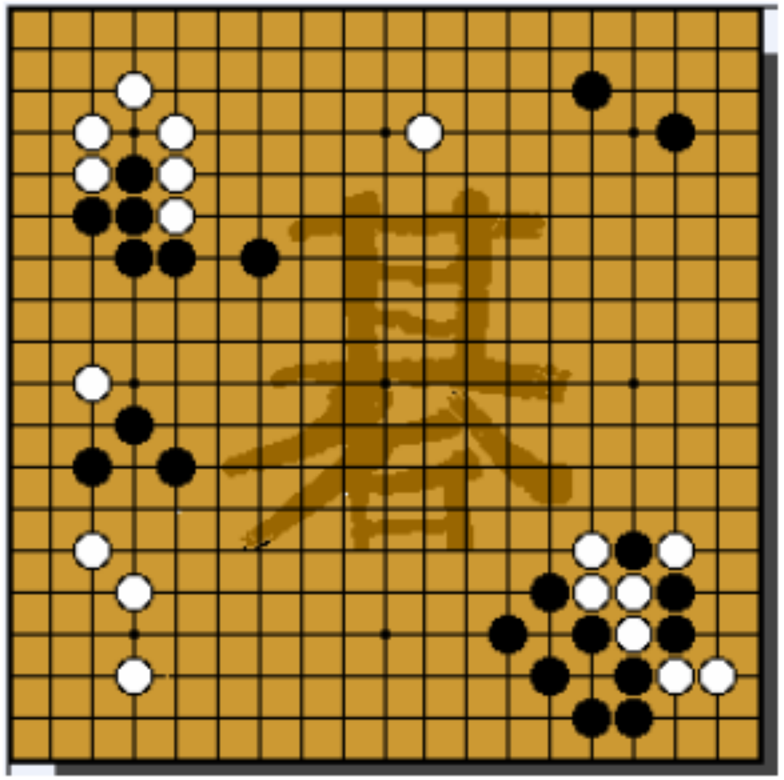


Figure 1 Go game

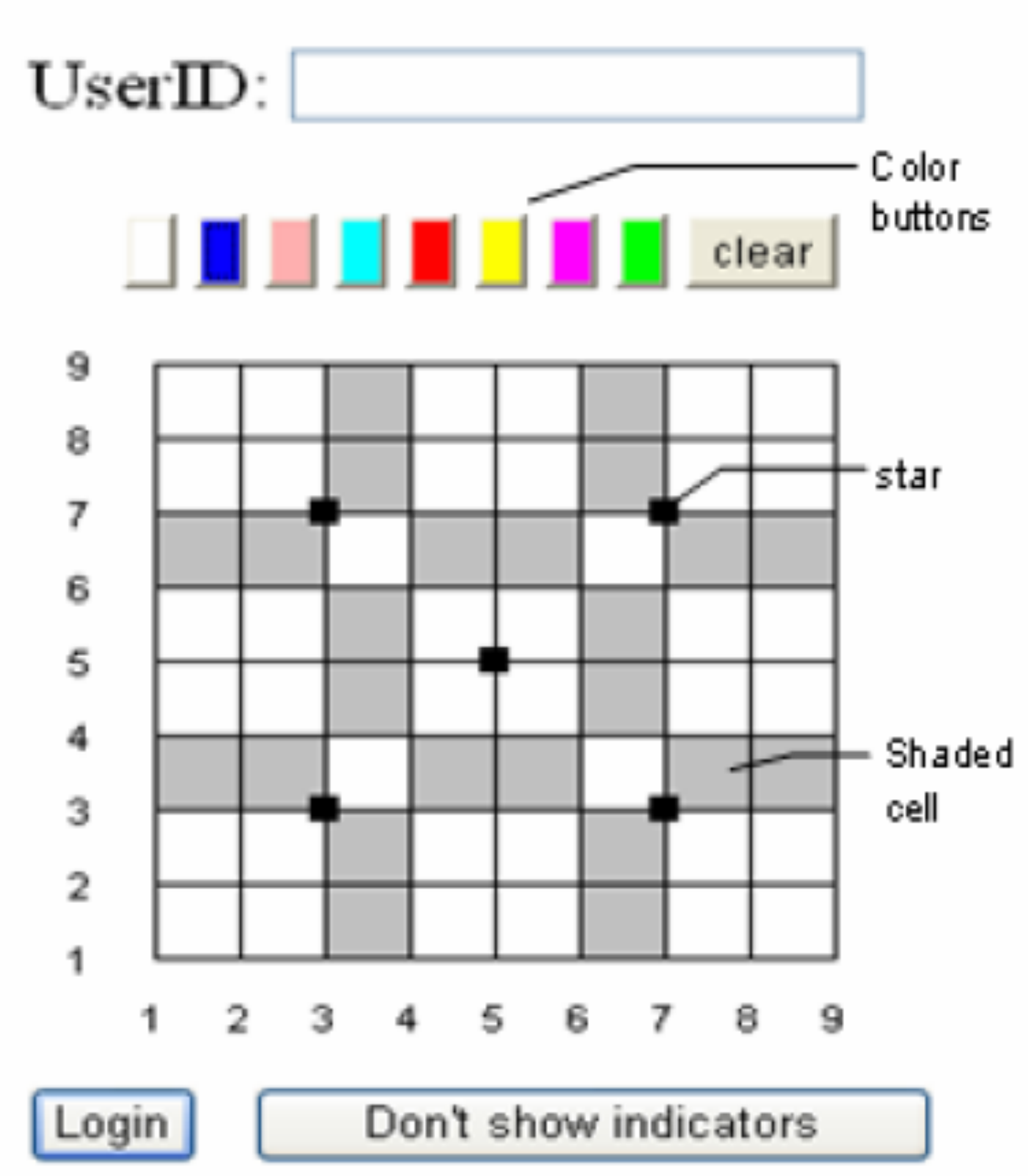
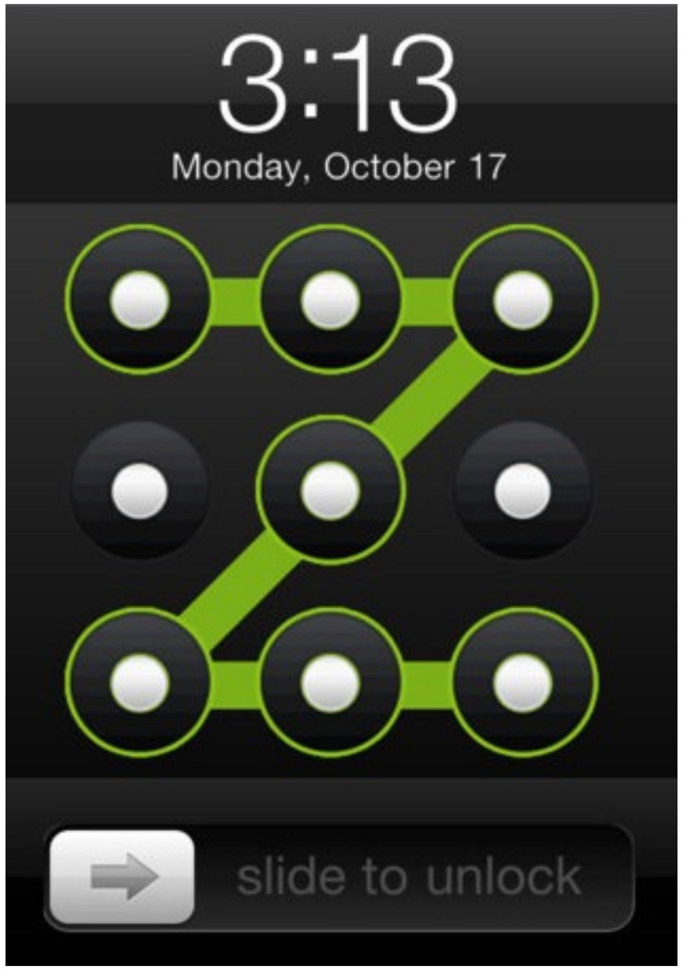
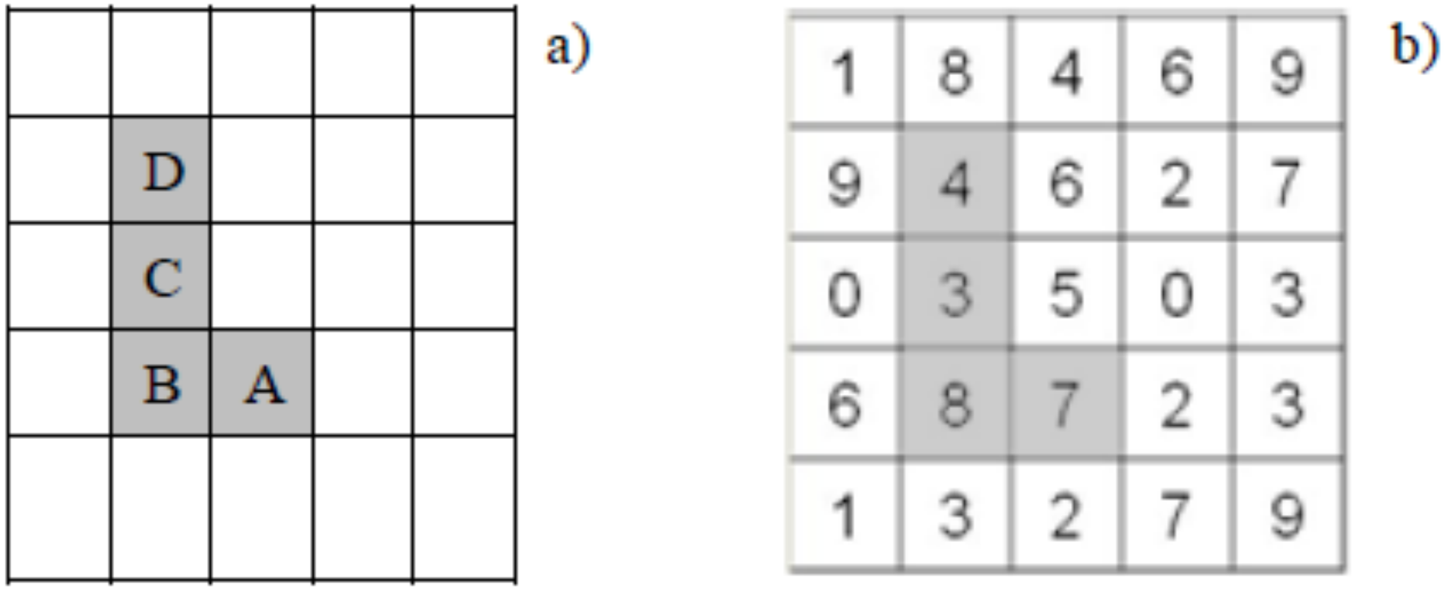


Figure 22 Main login interface

代表产品



PatternLock



a)

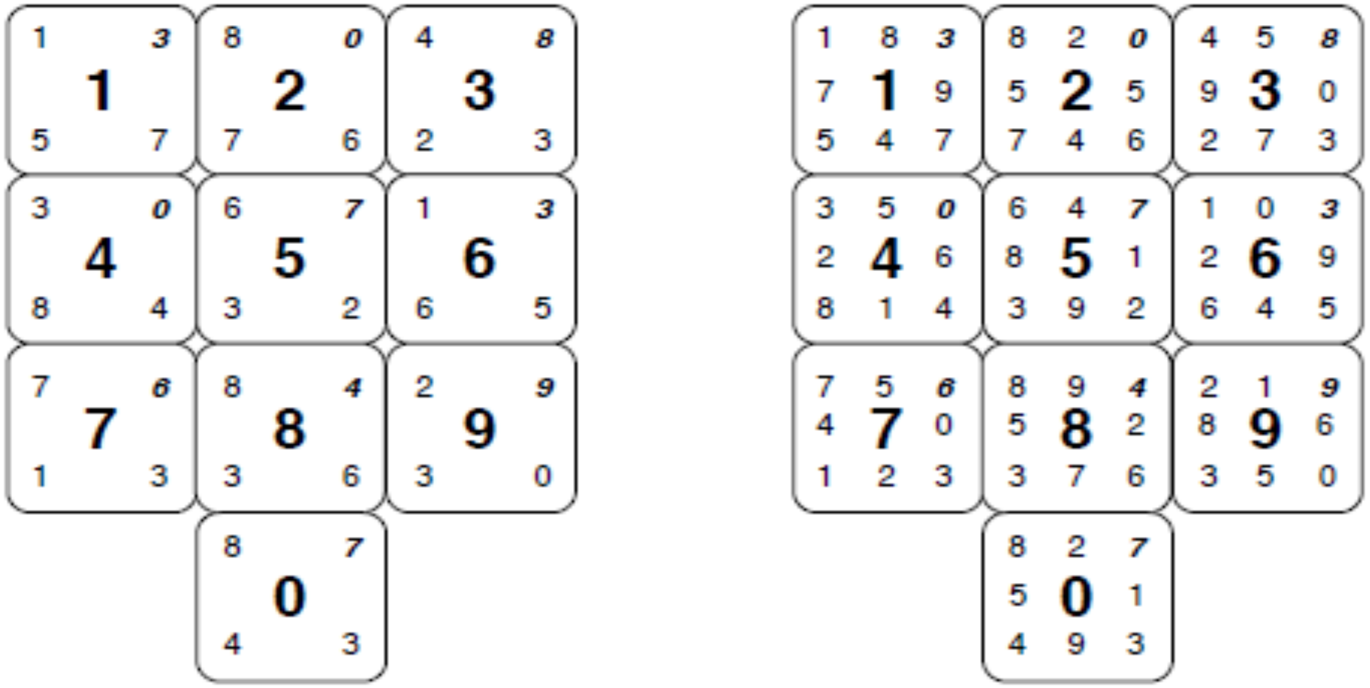
	D			
	C			
	B	A		

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) $k = 4$

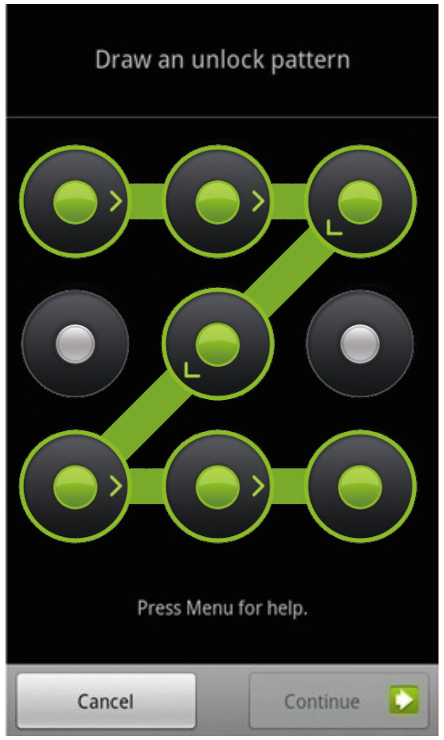
(b) $k = 8$

GridCode

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***


Draw an unlock pattern

Press Menu for help.

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

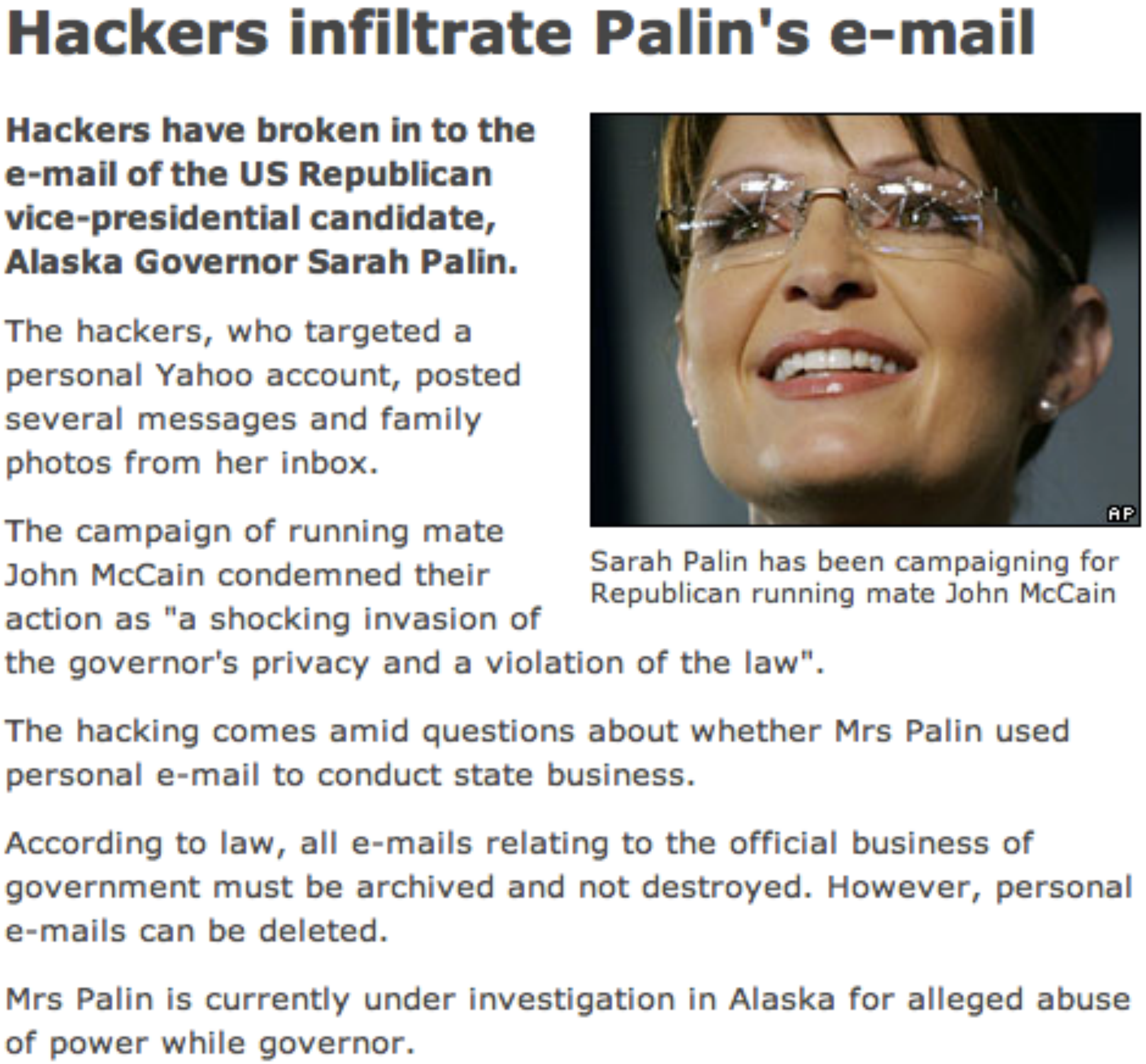
2008.09.17

gov.palin@yahoo.com

Where did you meet your spouse?

Wasilla High School

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.

Sarah Palin has been campaigning for Republican running mate John McCain

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.

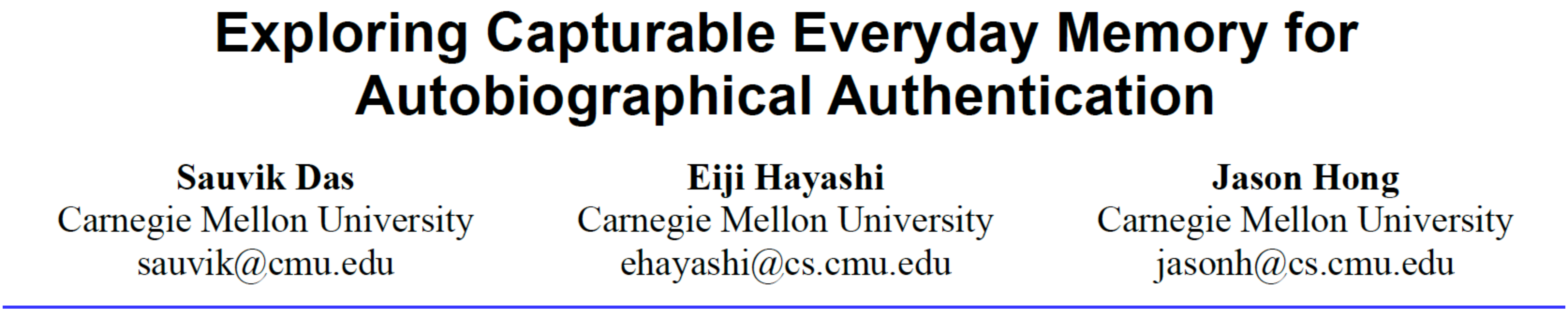
According to law, all e-mails relating to the official business of government must be archived and not destroyed. However, personal e-mails can be deleted.

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

http://wikileaks.org/wiki/VP_contender_Sarah_Palin_hacked

2008

自传体认证

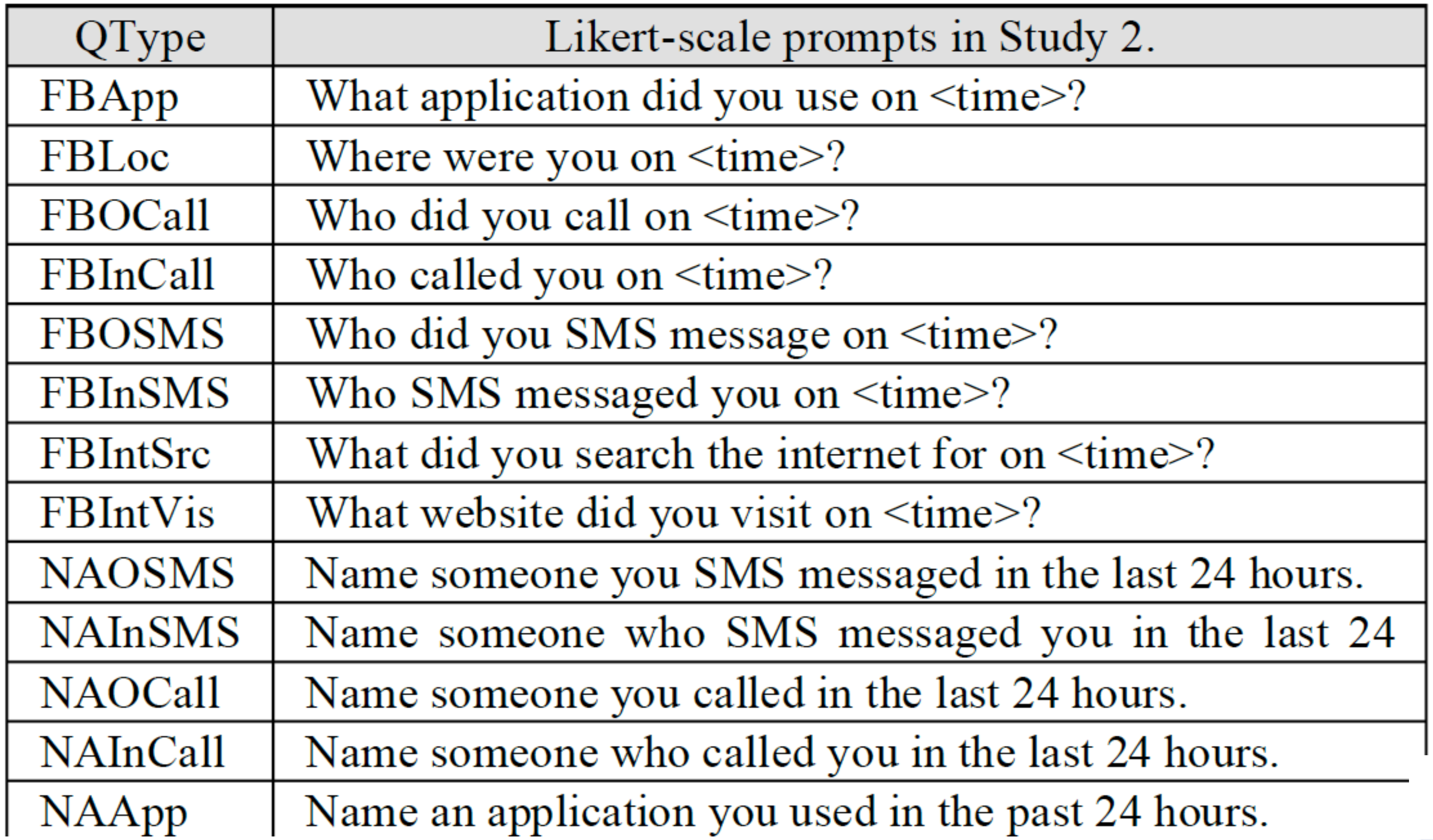


Exploring Capturable Everyday Memory for Autobiographical Authentication

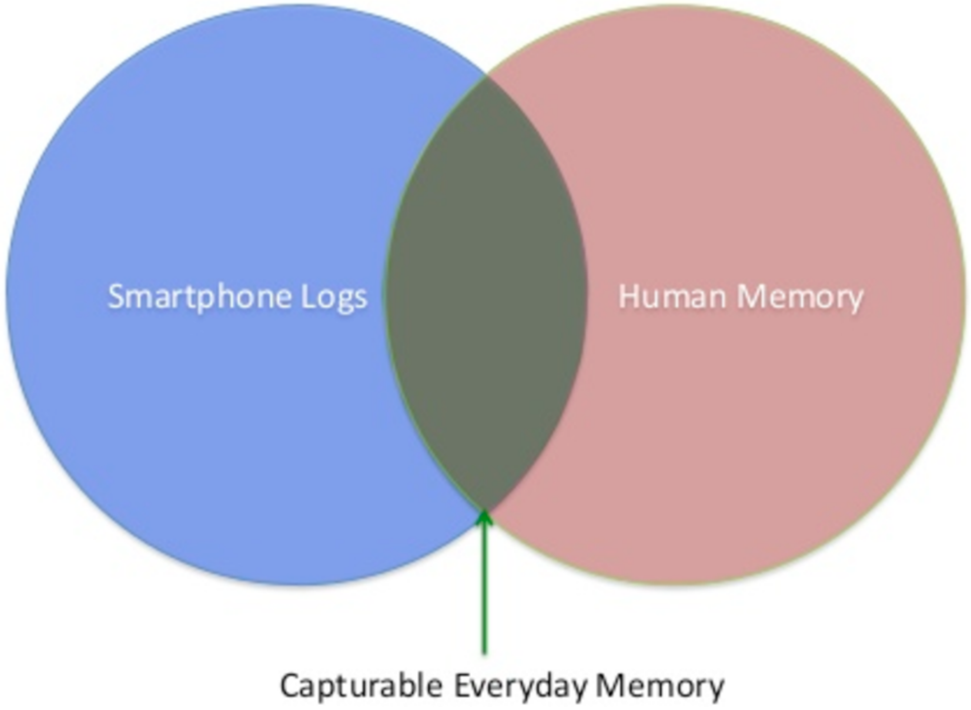
Sauvik Das
Carnegie Mellon University
sauvik@cmu.edu

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.

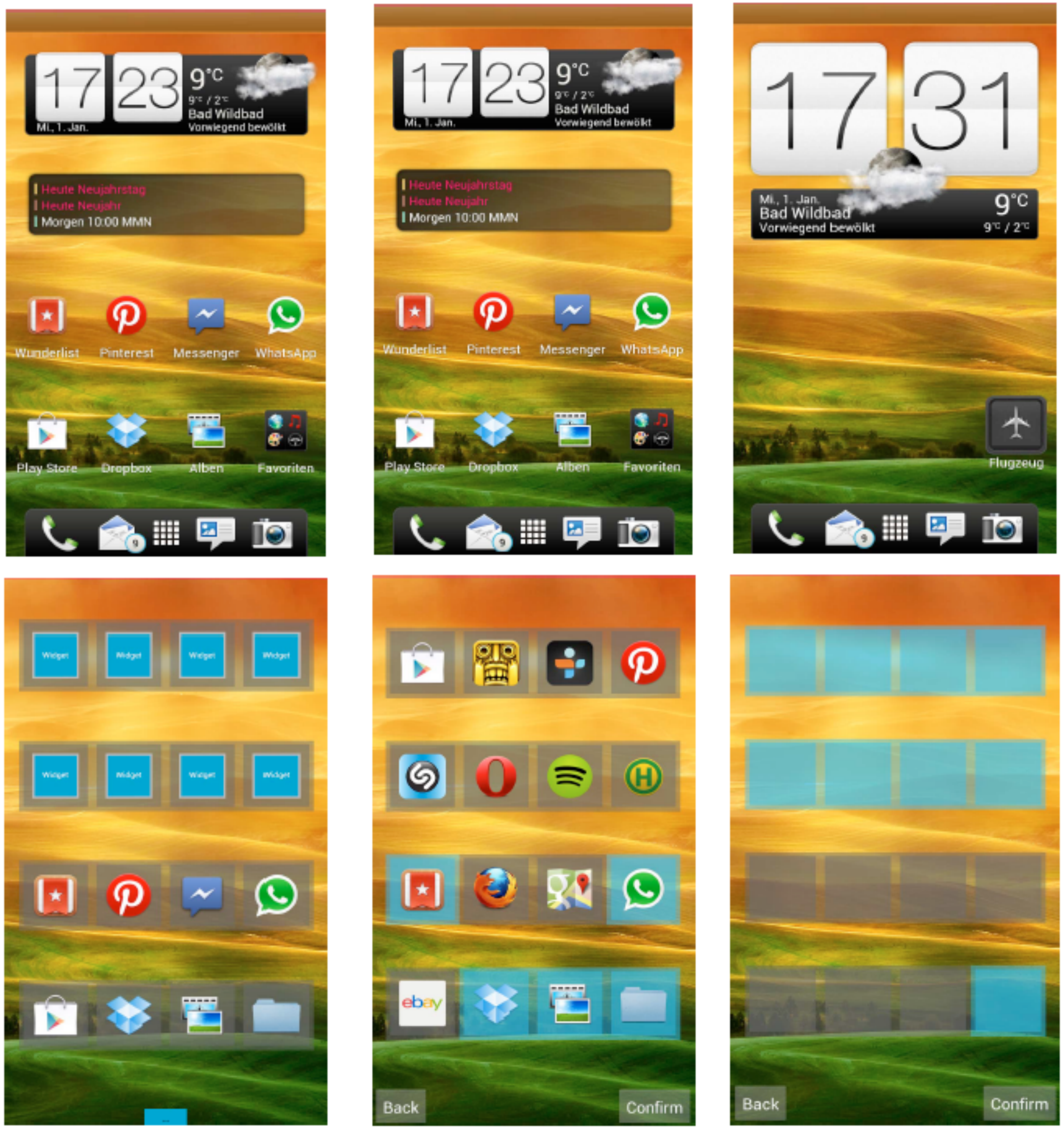


UBICOMP 2013
September 8-12
Zurich, Switzerland

http://sauvikdas.com/

PassApp

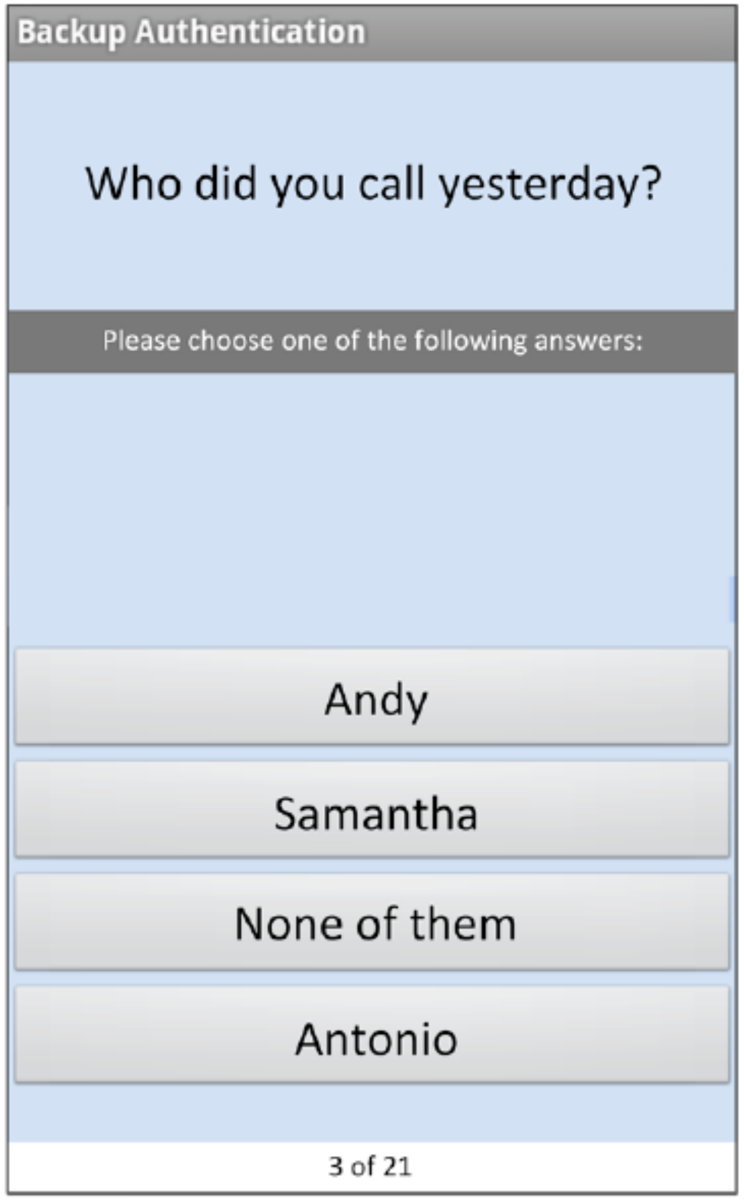
APP图标布局认证



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:

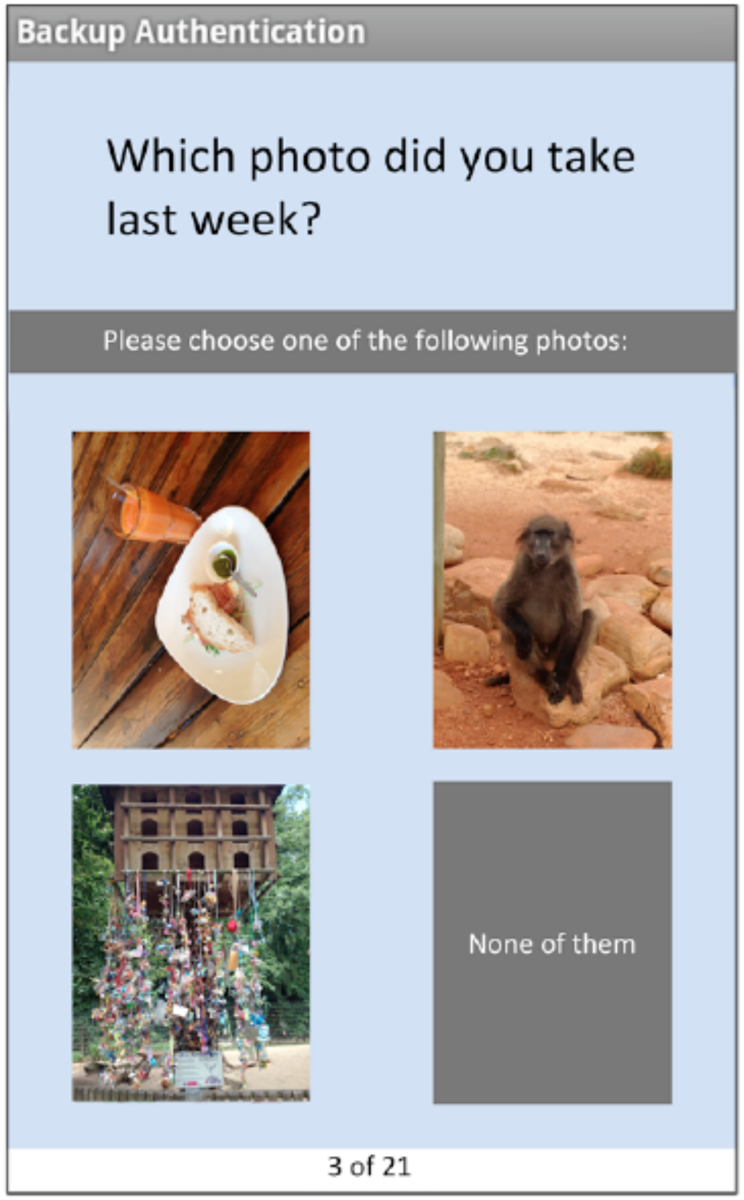
Andy

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

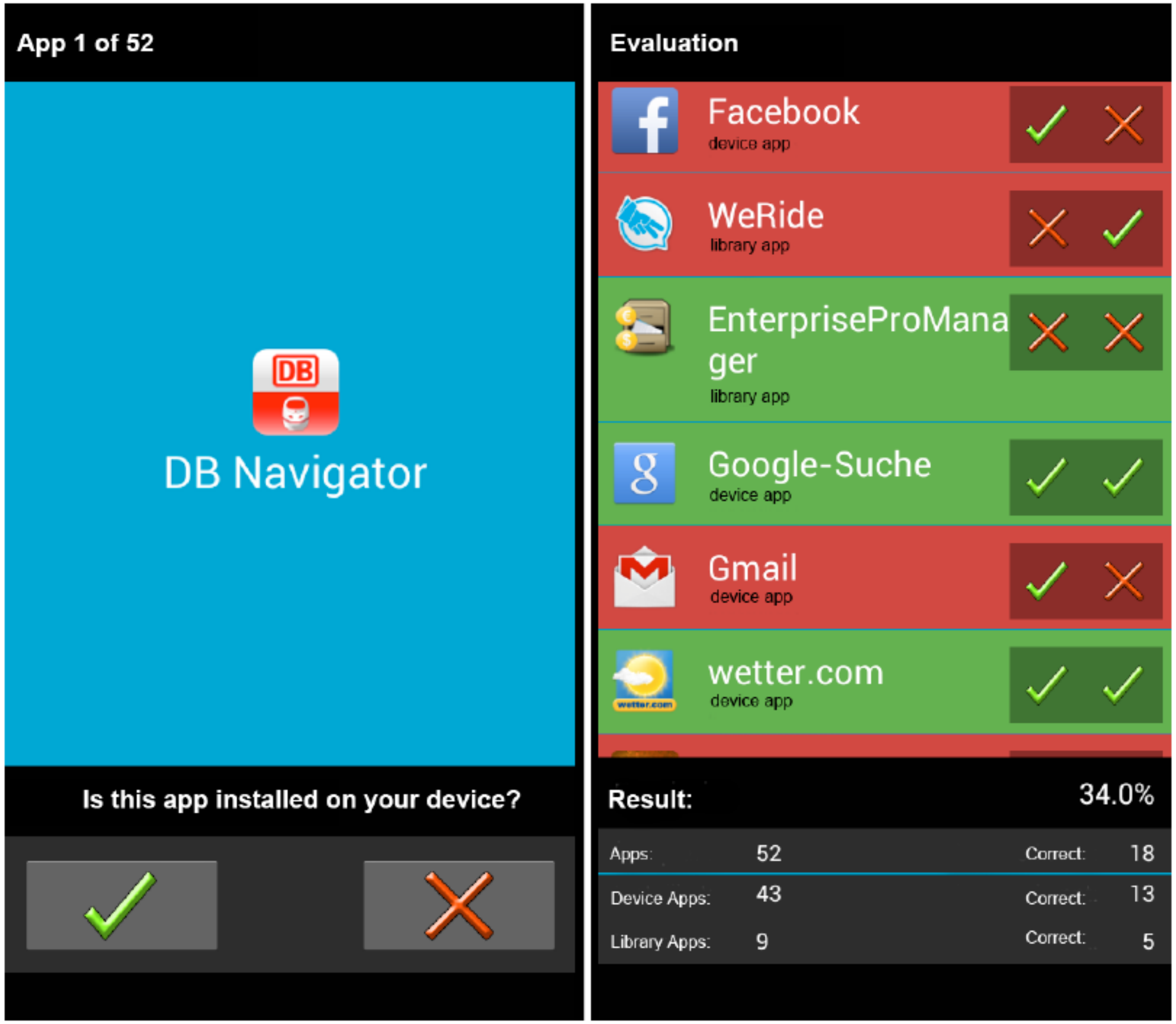
Category	Question + Timespan
SMS (out)	Who did you text [Y | LW]?
SMS (in)	Who texted you [Y | LW]?
Call (out)	Who did you call [Y | LW]?
Call (in)	Who called you [Y | LW]?
App	Which App did you use [Y | LW]?
App Install	Which app did you install/update [Y | LW]?
Photos	Which photo did you take [Y |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



App 1 of 52

DB Navigator

Is this app installed on your device?

✓ ✗

Evaluation

Facebook	device app	✓	✗
WeRide	library app	✗	✓
EnterpriseProManager	library app	✗	✗
Google-Suche	device app	✓	✓
Gmail	device app	✓	✗
wetter.com	device app	✓	✓

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

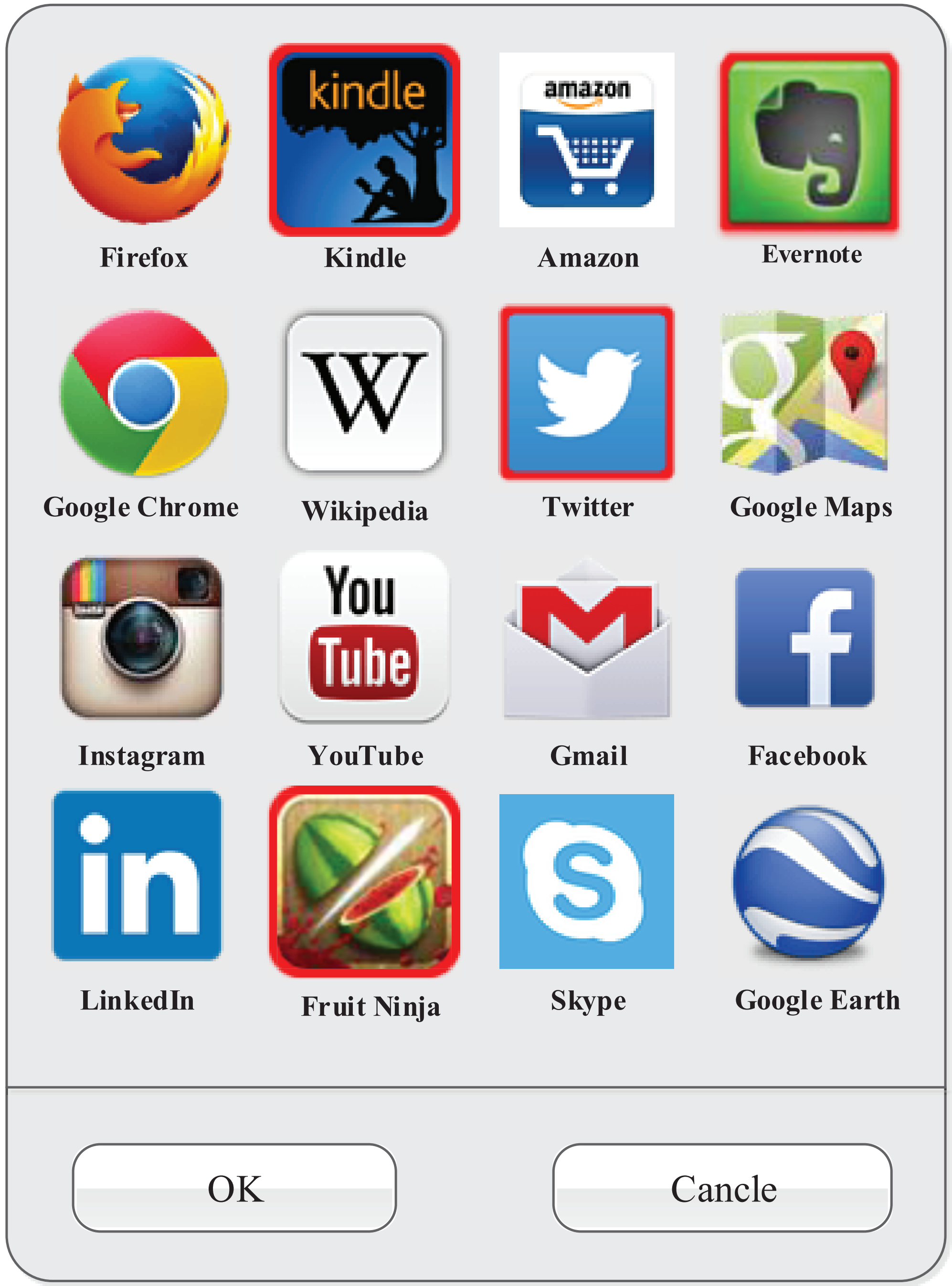
PassApp

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

installed apps

on their mobile devices

as password



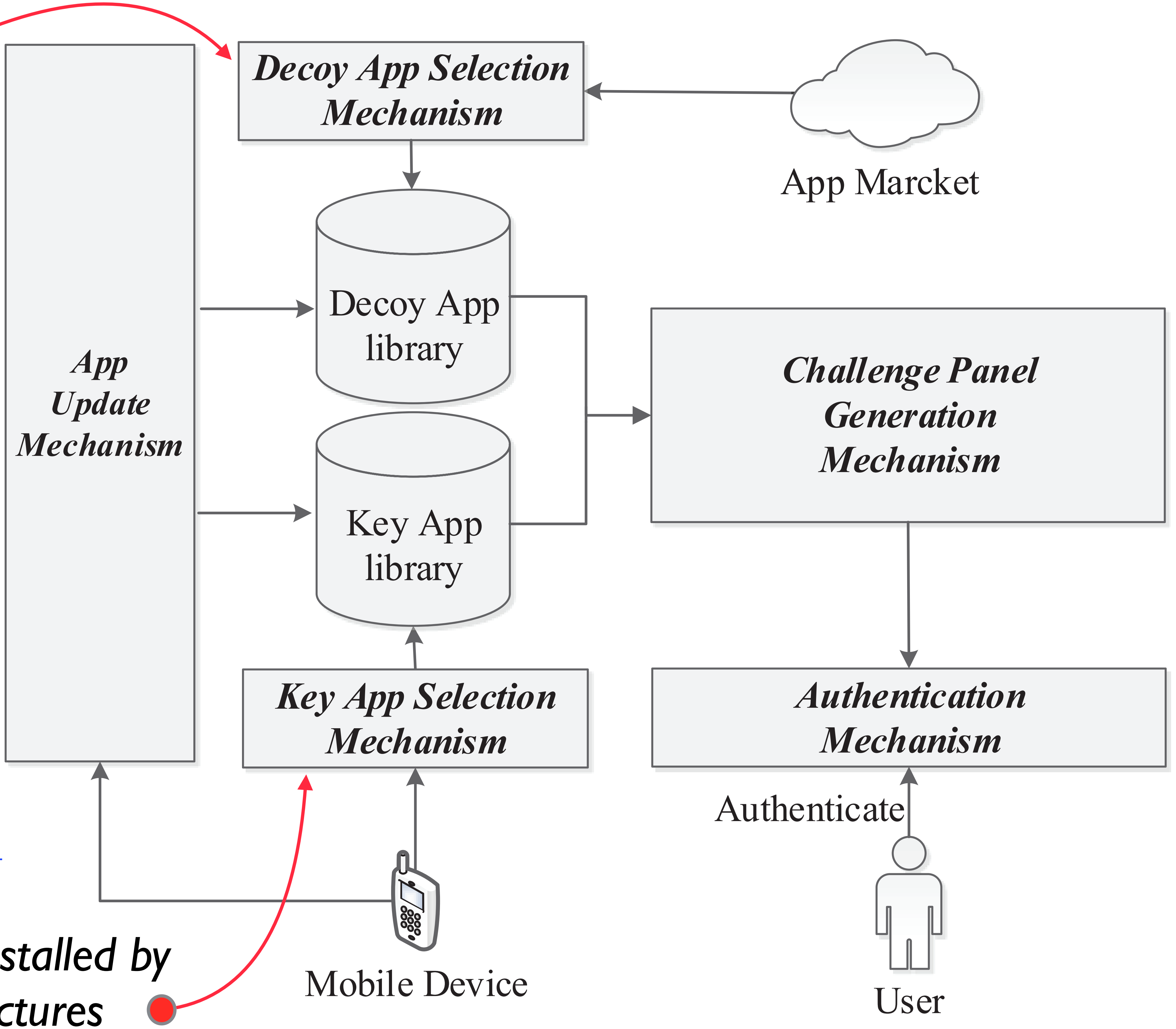
PassApp Mechanism

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*

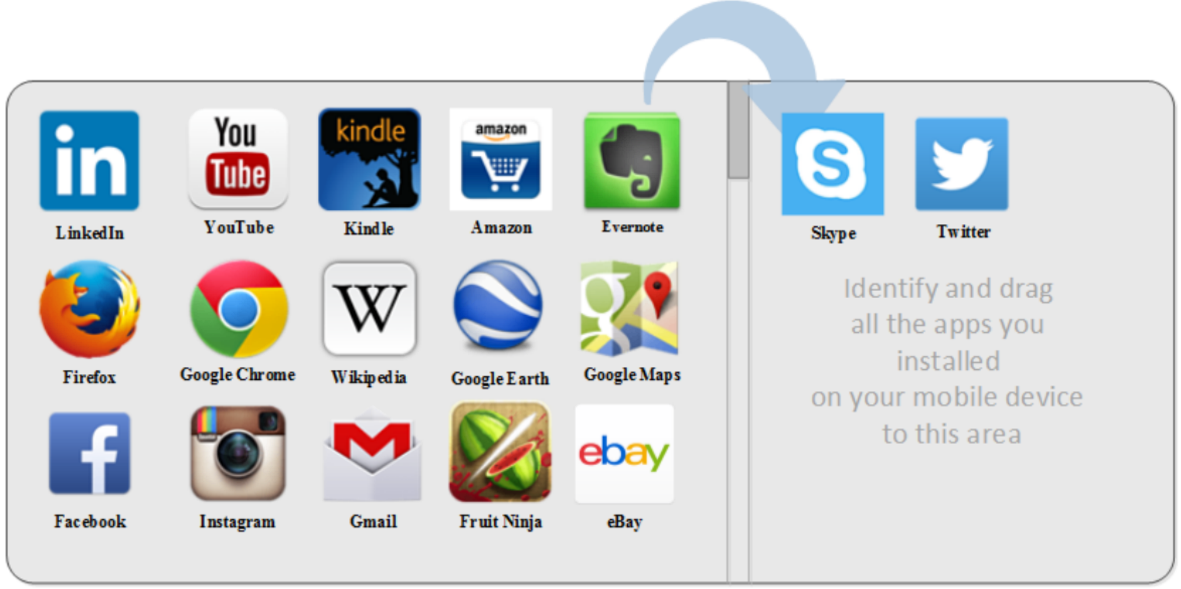
rule out the apps preinstalled by device and OS manufactures



User Study

Day 1

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

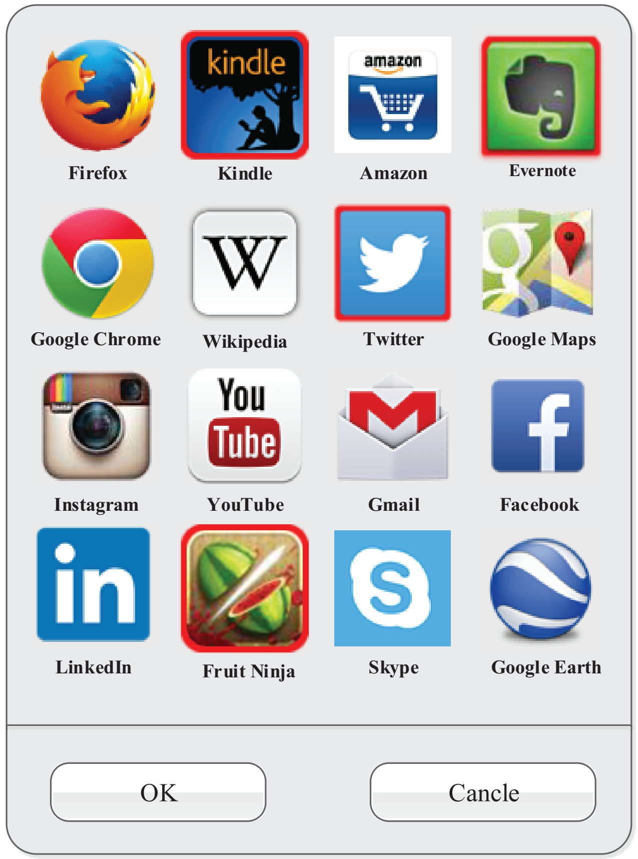


Identify and drag all the apps you installed on your mobile device to this area

42 participants

Day 2

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



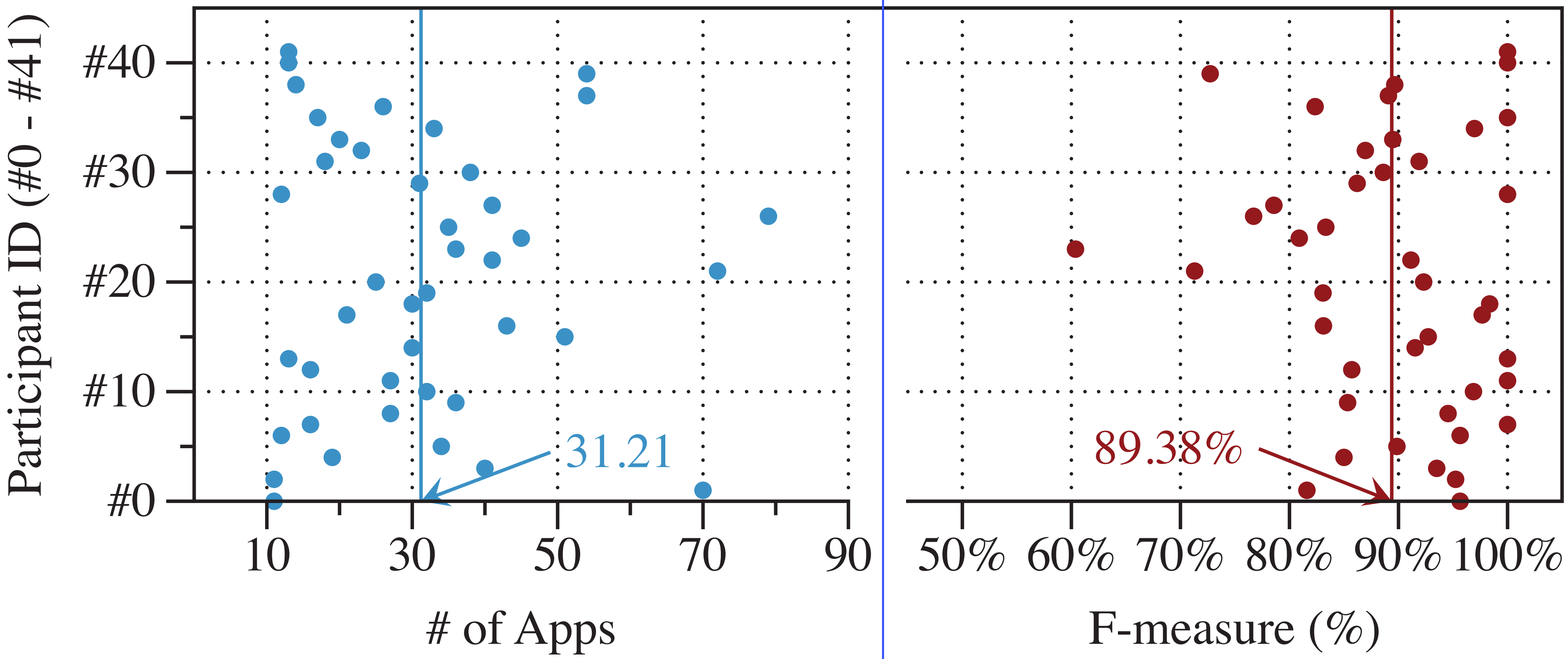
unlock10 times

42 *10

Login Time

Success Rate

Memory about Installed Apps



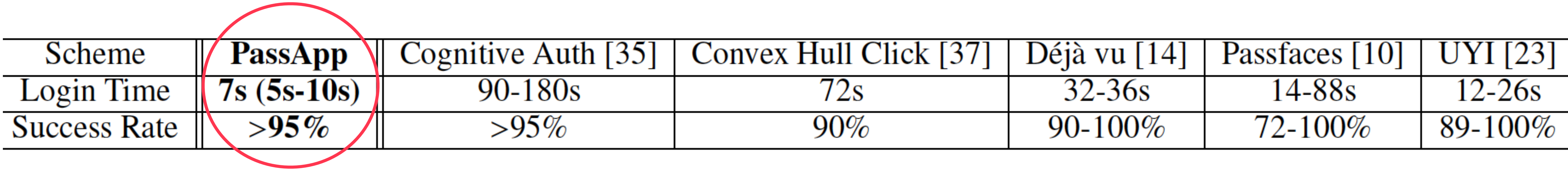
Max:79, Min: 11, SD: 16.79

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

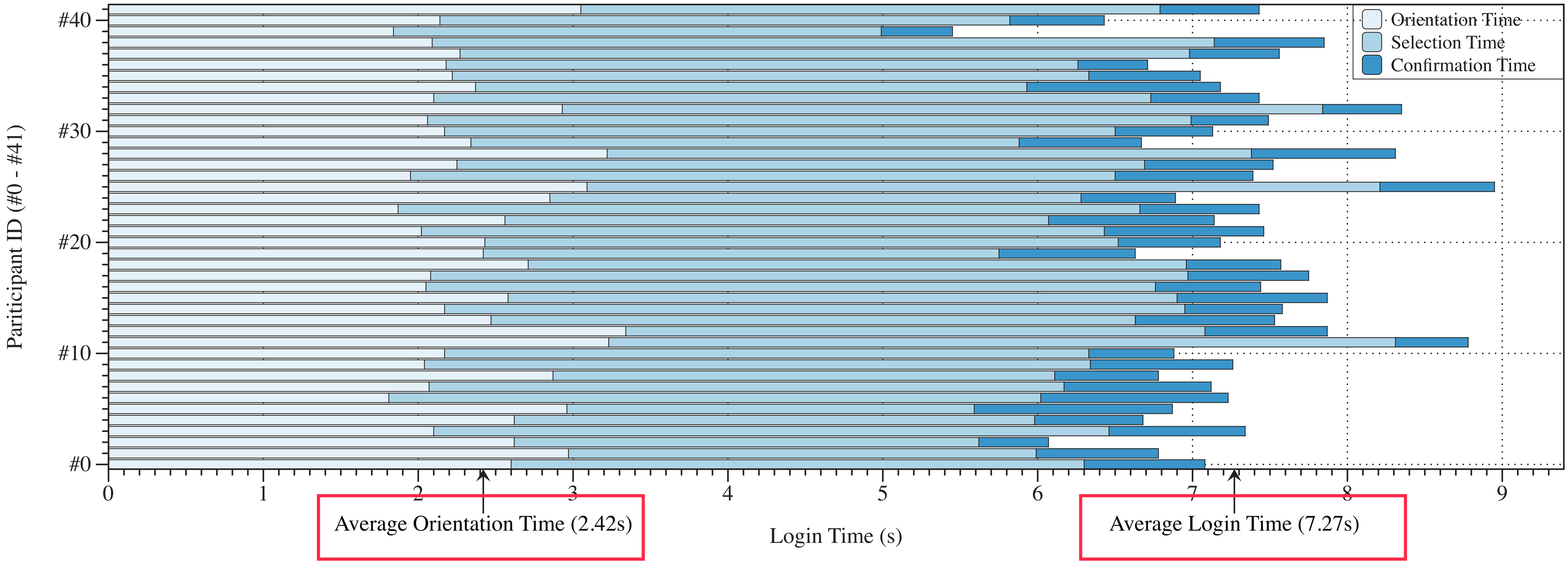
$$P(precision) = \frac{\sum picked\ installed\ apps}{\sum all\ apps\ picked} \qquad R(recall) = \frac{\sum picked\ installed\ apps}{\sum all\ installed\ apps}$$

PassApp

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%



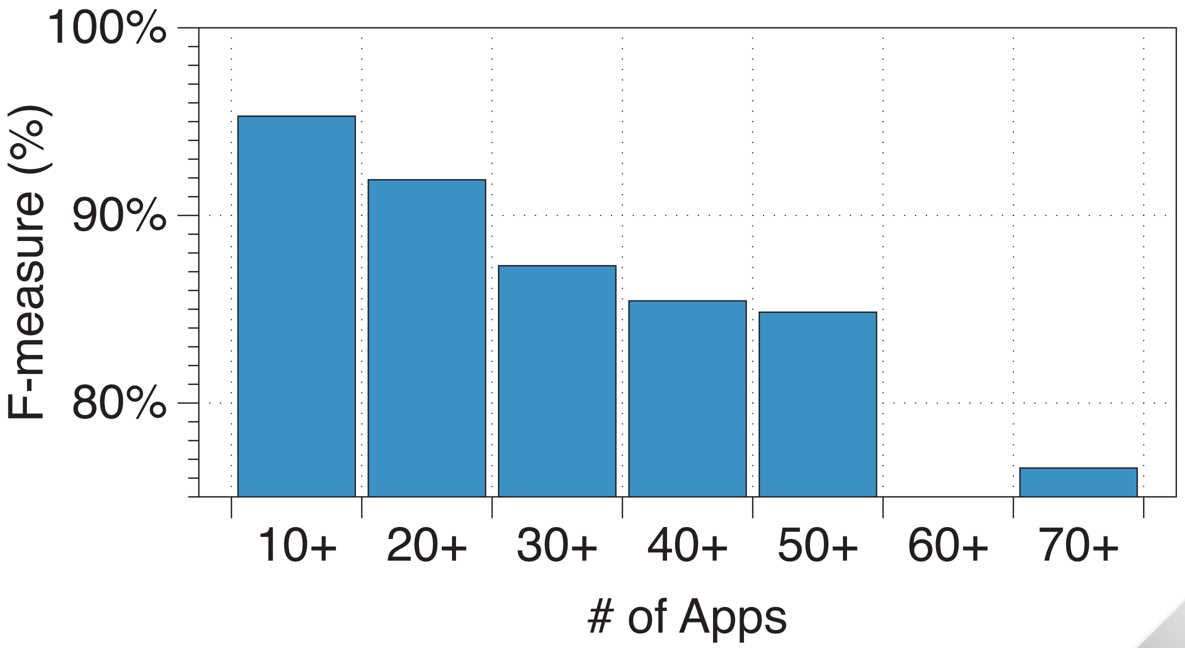
Average Orientation Time (2.42s)

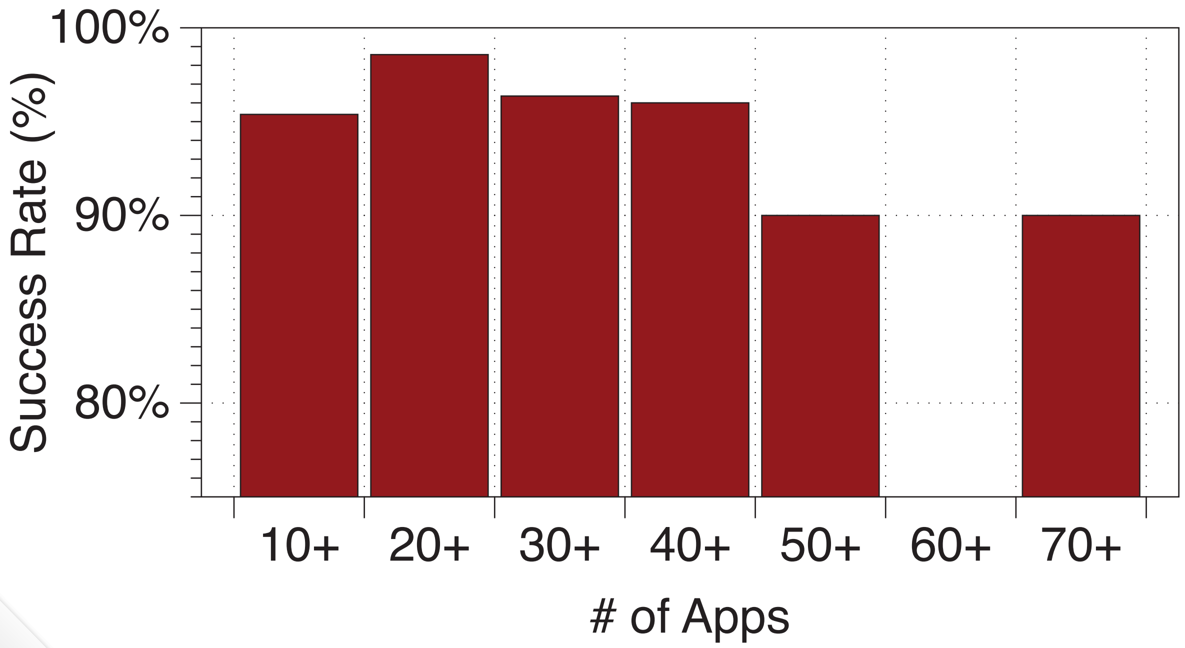
Average Login Time (7.27s)

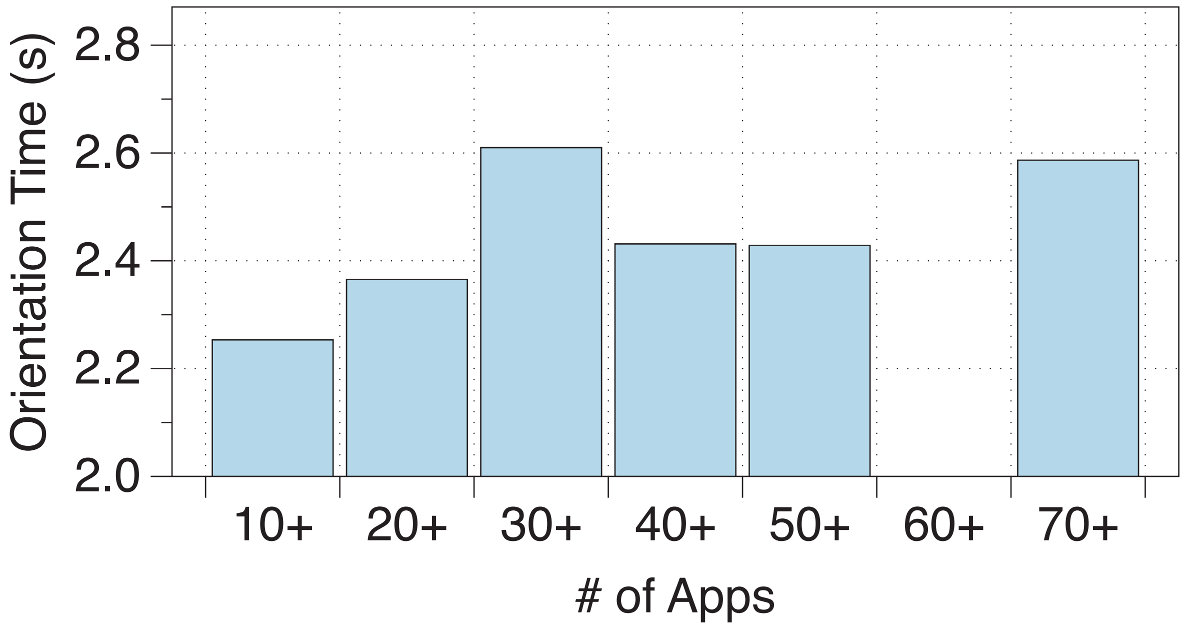
Average confirmation time: 0.76s

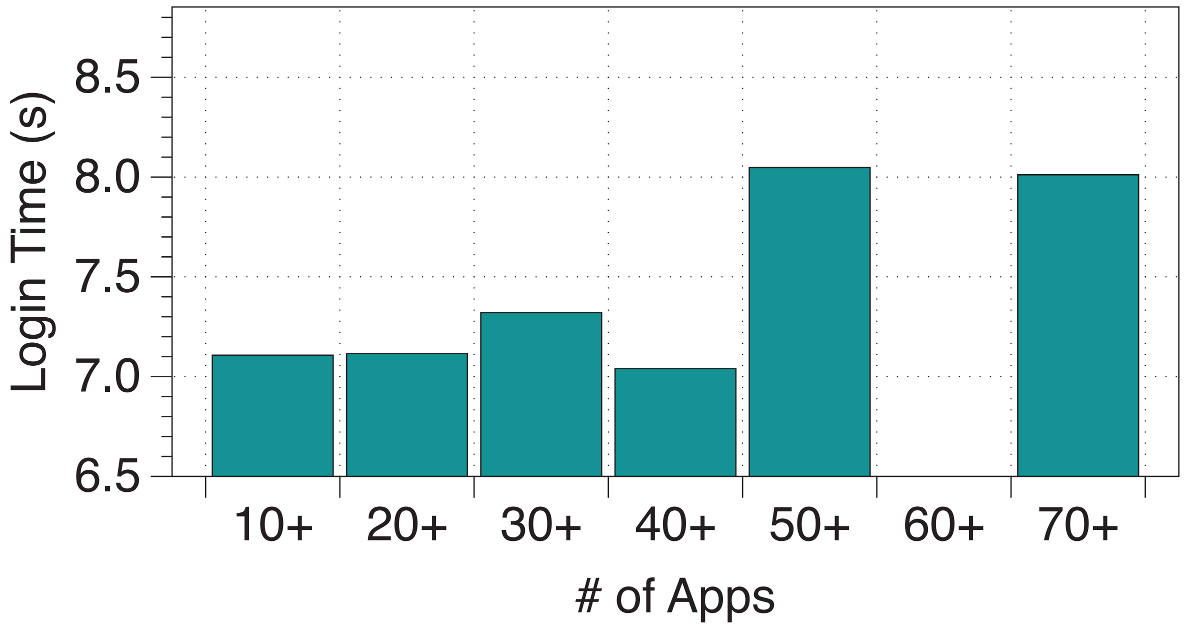
PassApp

Number of Key Apps & Usability Indices



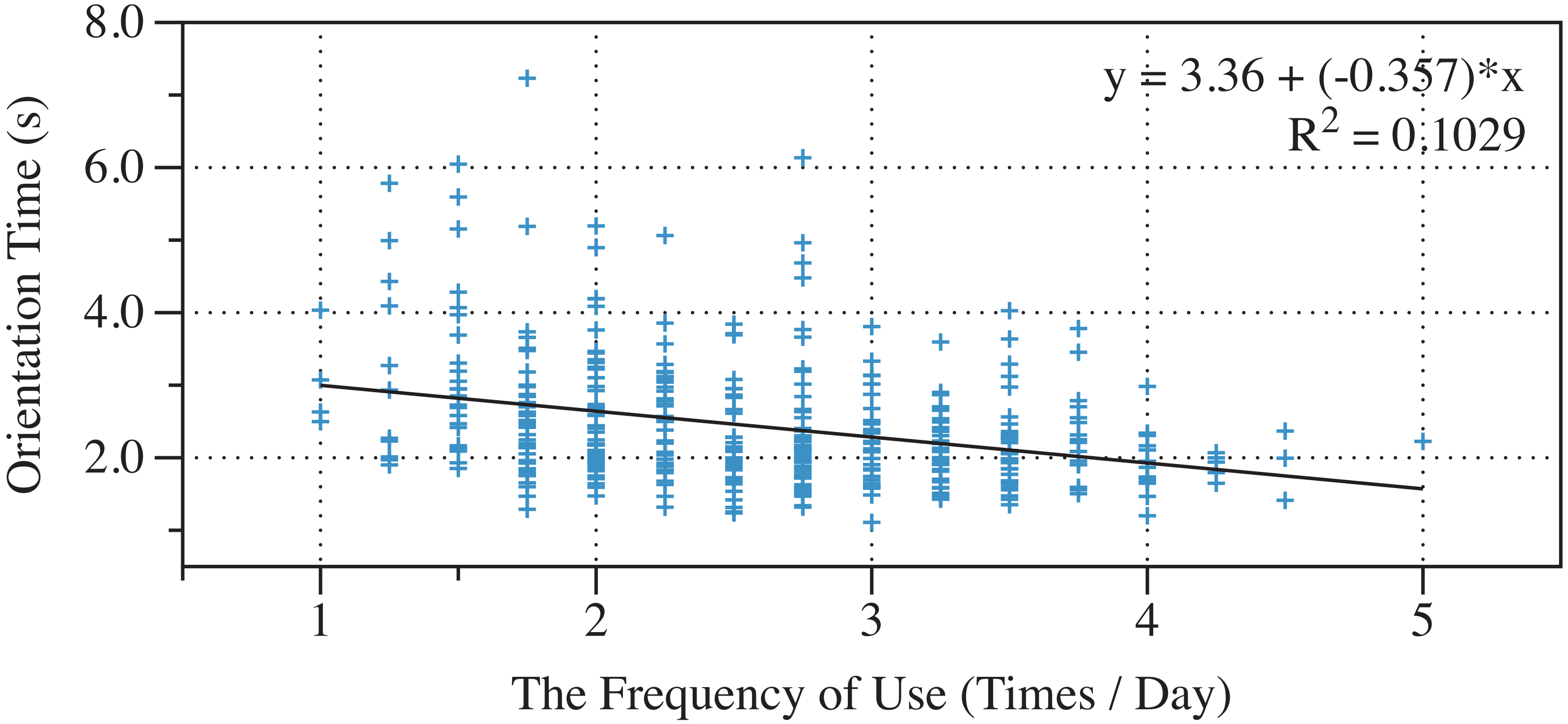






PassApp

Frequency of Using Apps & Usability Indices



28.38% <0.2times/days

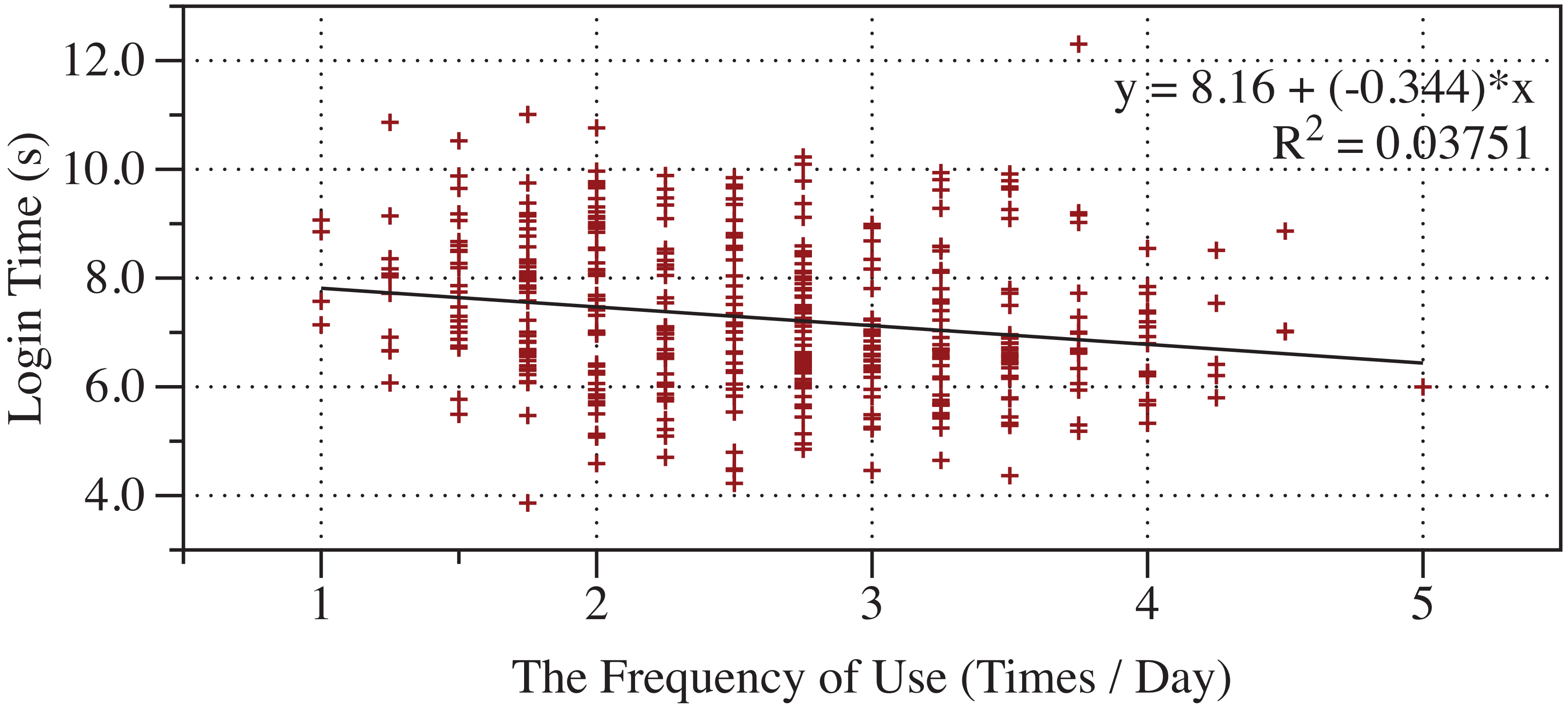
21.66% 0.2 -0.5 t/d

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



PassApp

Security Analysis

Brutal-force Attacks

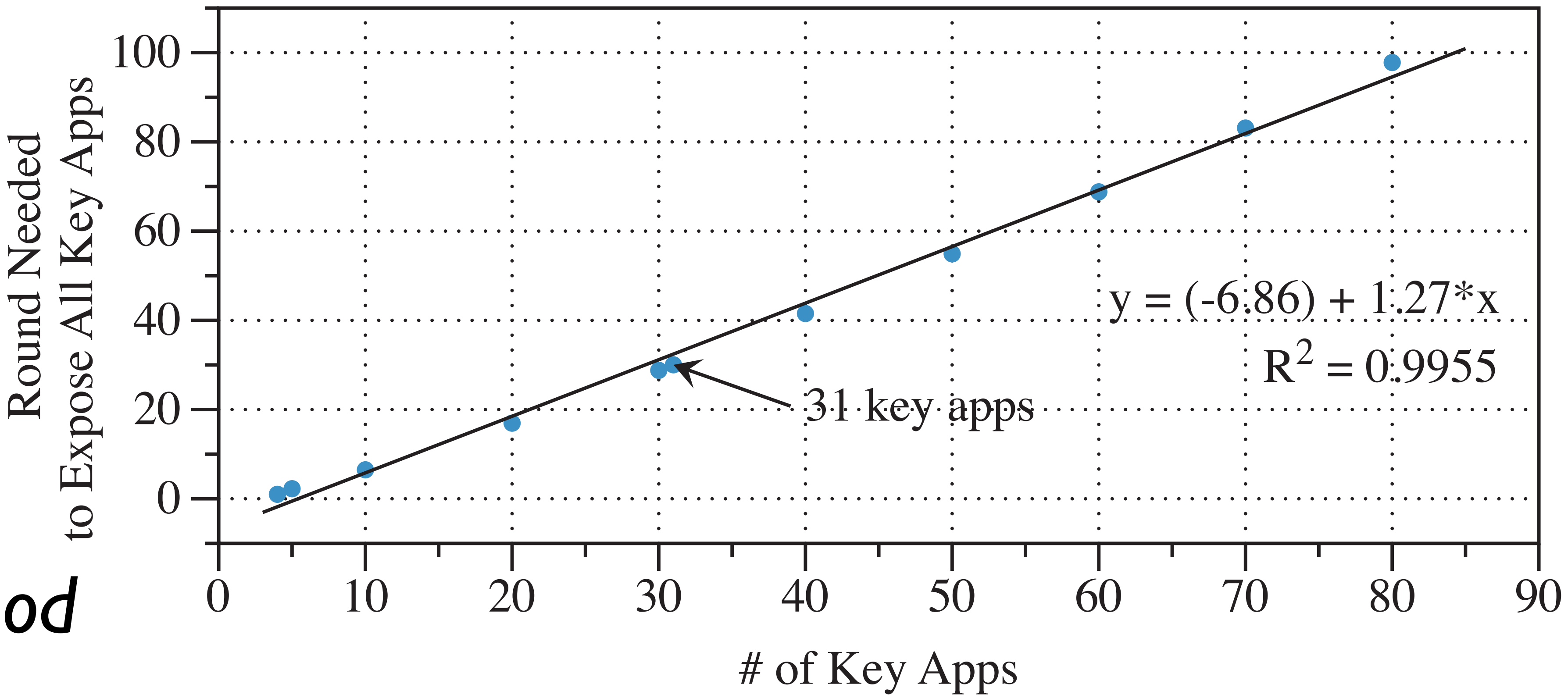
$$1/\binom{16}{4} = 1/1820.$$

$\boxed{0.055\%}$

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



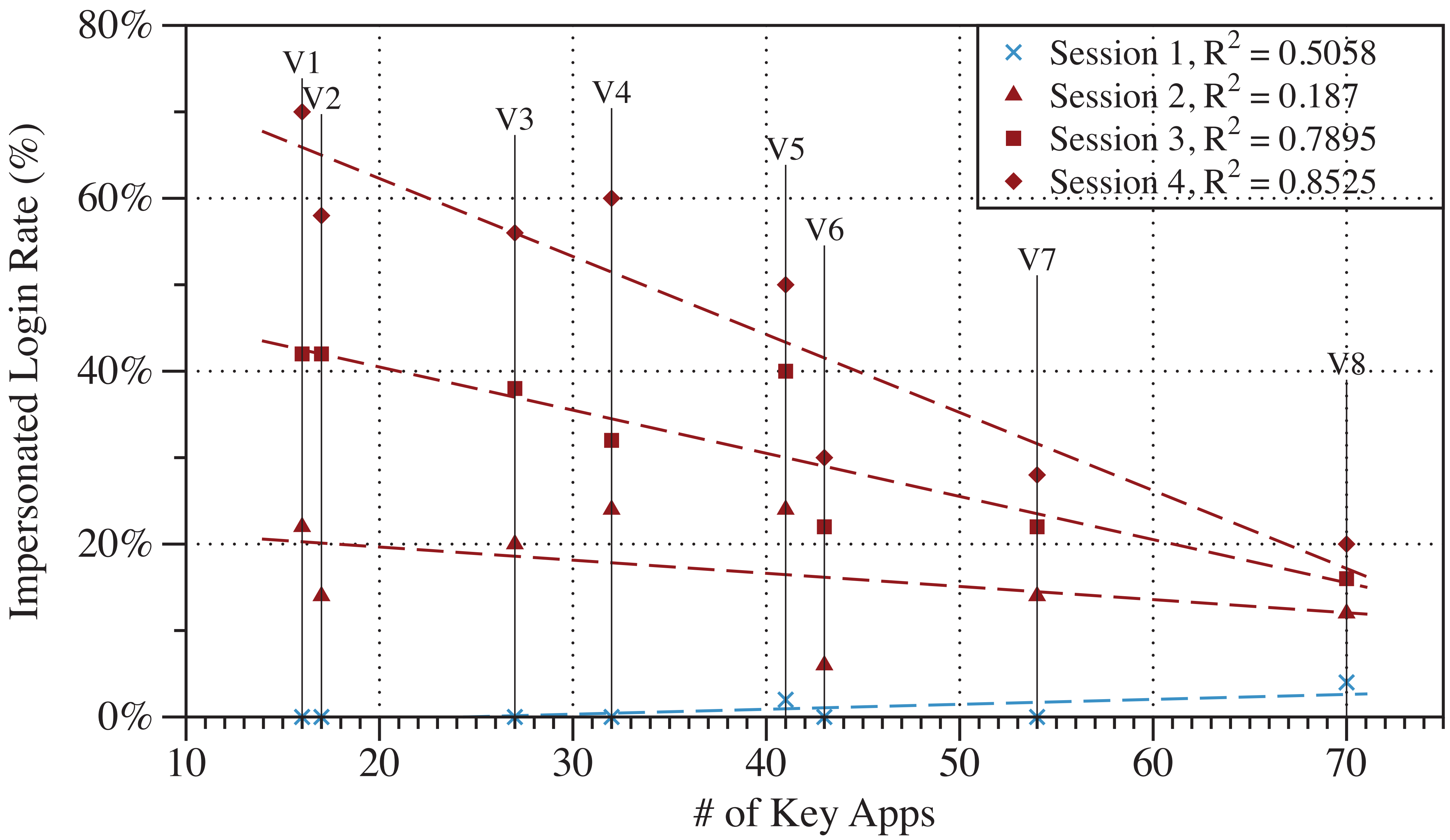
Monte Carlo Method

PassApp

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

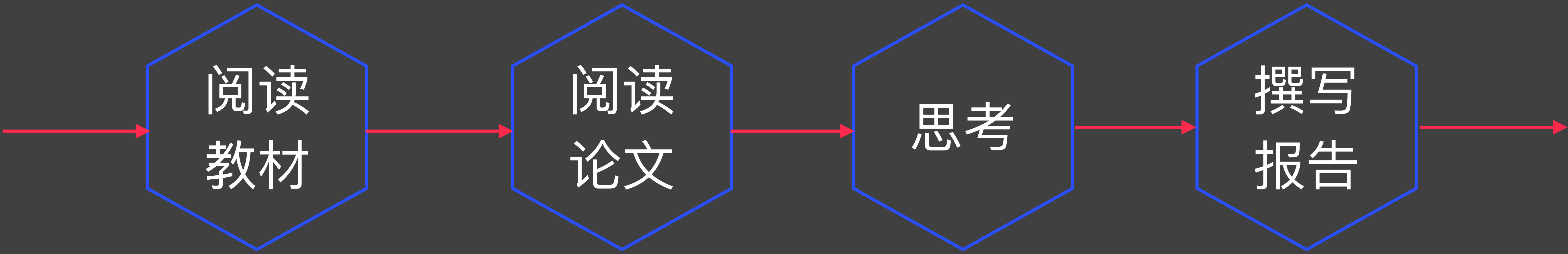
- *Key app selection*
  - ✴ *too short or too many, popular apps, communication apps*
- *Decoy app selection*
  - ✴ *app market, device manufacture, OS, language,etc*
- *Challenge panel generation (n key * m decoy * r rounds)*
- *Login time (challenge, backup authentication)*
- *Participant (field study 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)*

提问时间！

课后作业



阅读教材

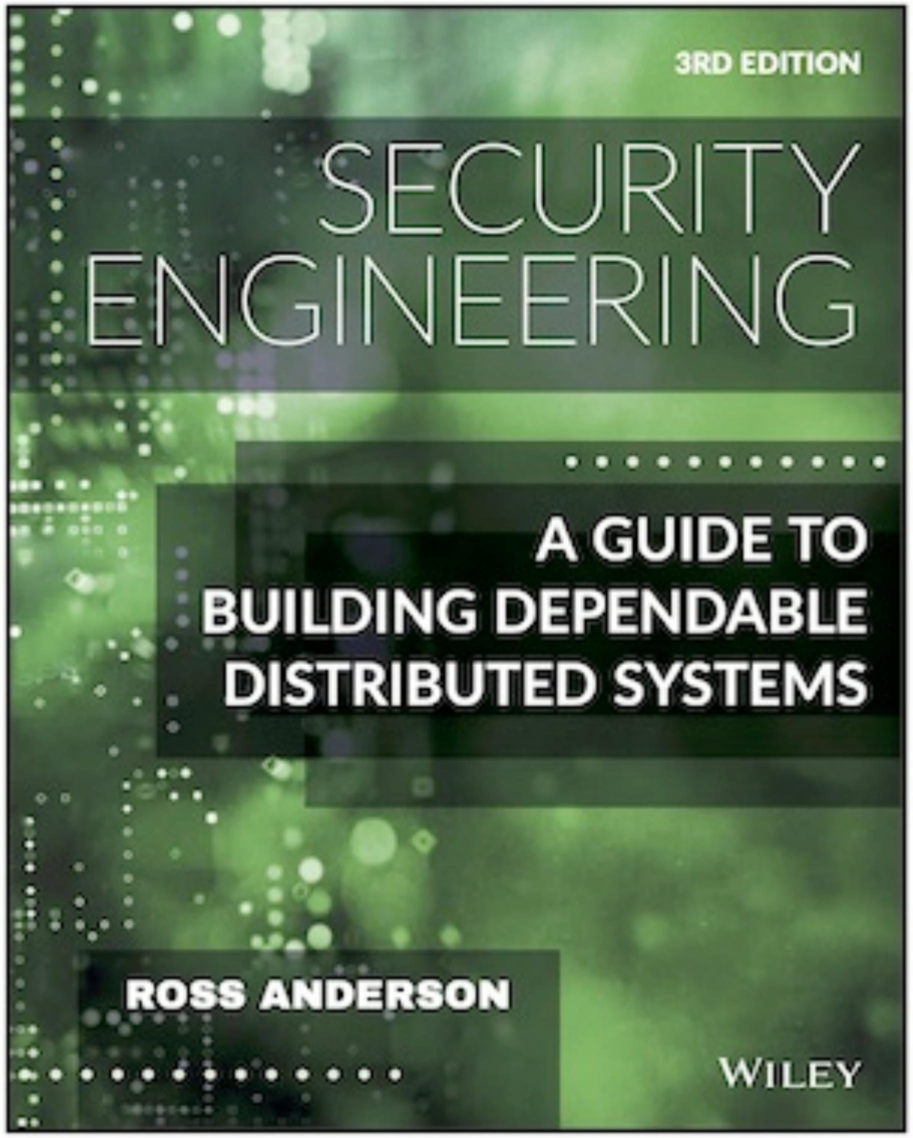
阅读论文

思考

撰写报告

Homework

阅读教材



3RD EDITION

SECURITY ENGINEERING

A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS

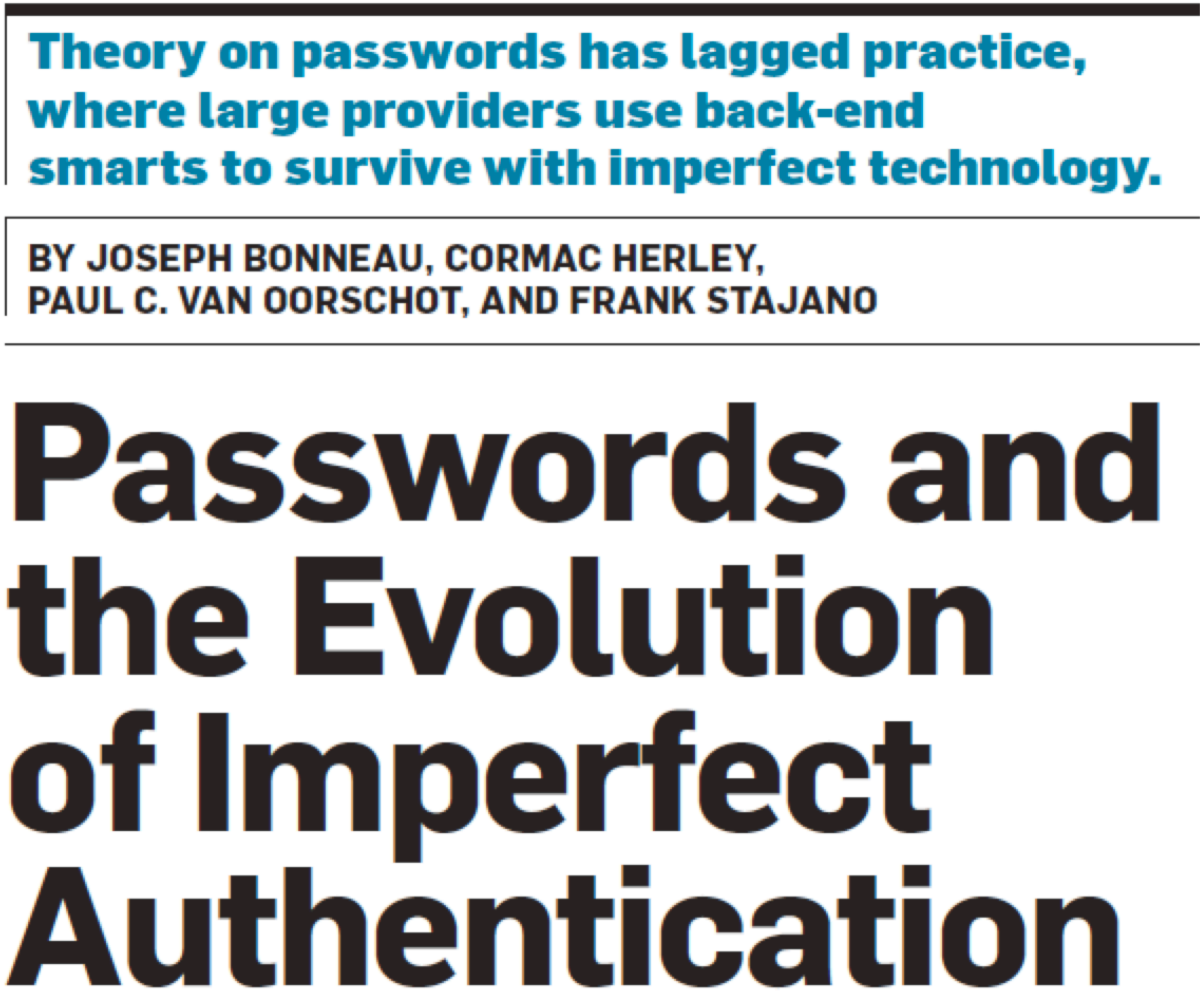
ROSS ANDERSON

WILEY

阅读第三章
有余力的可以看看第二章

Homework 课后作业

要求阅读如下论文，写论文阅读报告



Theory on passwords has lagged practice, where large providers use back-end smarts to survive with imperfect technology.

BY JOSEPH BONNEAU, CORMAC HERLEY, PAUL C. VAN OORSCHOT, AND FRANK STAJANO

Passwords and the Evolution of Imperfect Authentication

Communication of ACM 2015

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

引用该论文的

周日晚上12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io