MobileHCI 2015
August 24th – August 27th 2015
Copenhagen, Denmark

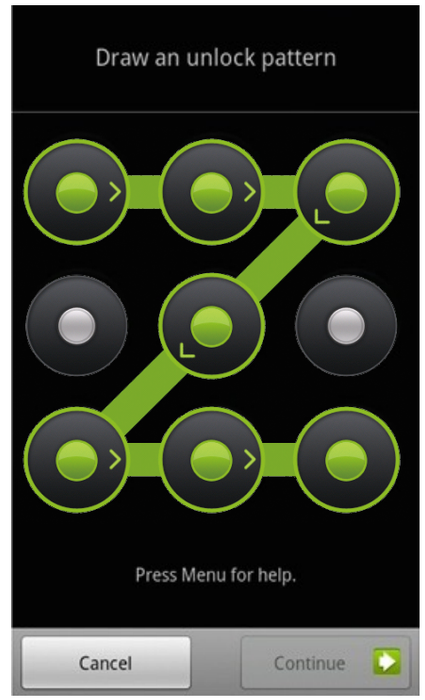
My App is My Password!

Huiping Sun, Ke Wang, Xu Li, Nan Qin, Zhong Chen

Peking University

Backgrounds

- *Graphical Password*
  - ✳ *more applicable on mobile devices than text passwords*
  - ✳ *vulnerable to shoulder surfing attacks*
  - ✳ ***most existing graphical password schemes require users to actively memorize passwords***



Graphical passwords based on existing memory

- *Authentication based on existing memory*
  - ✳ *weak passwords*
  - ✳ *security questions*
  - ✳ *dynamic security questions*
  - ✳ *autobiographical authentication*

PassApp Concept

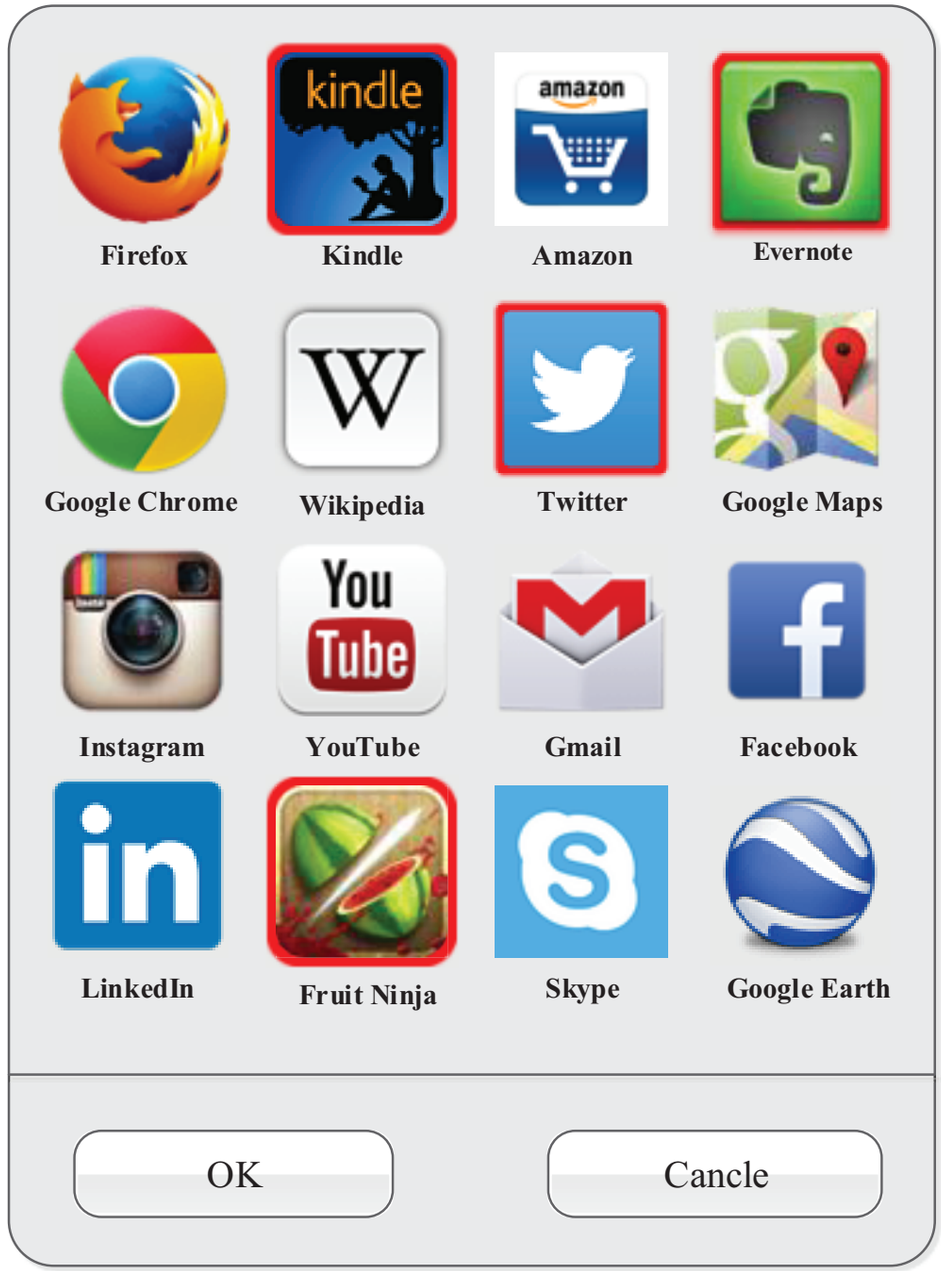
PassApp

is a novel recognition-based graphical password which utilizes users'

installed apps

on their mobile devices

as passwords



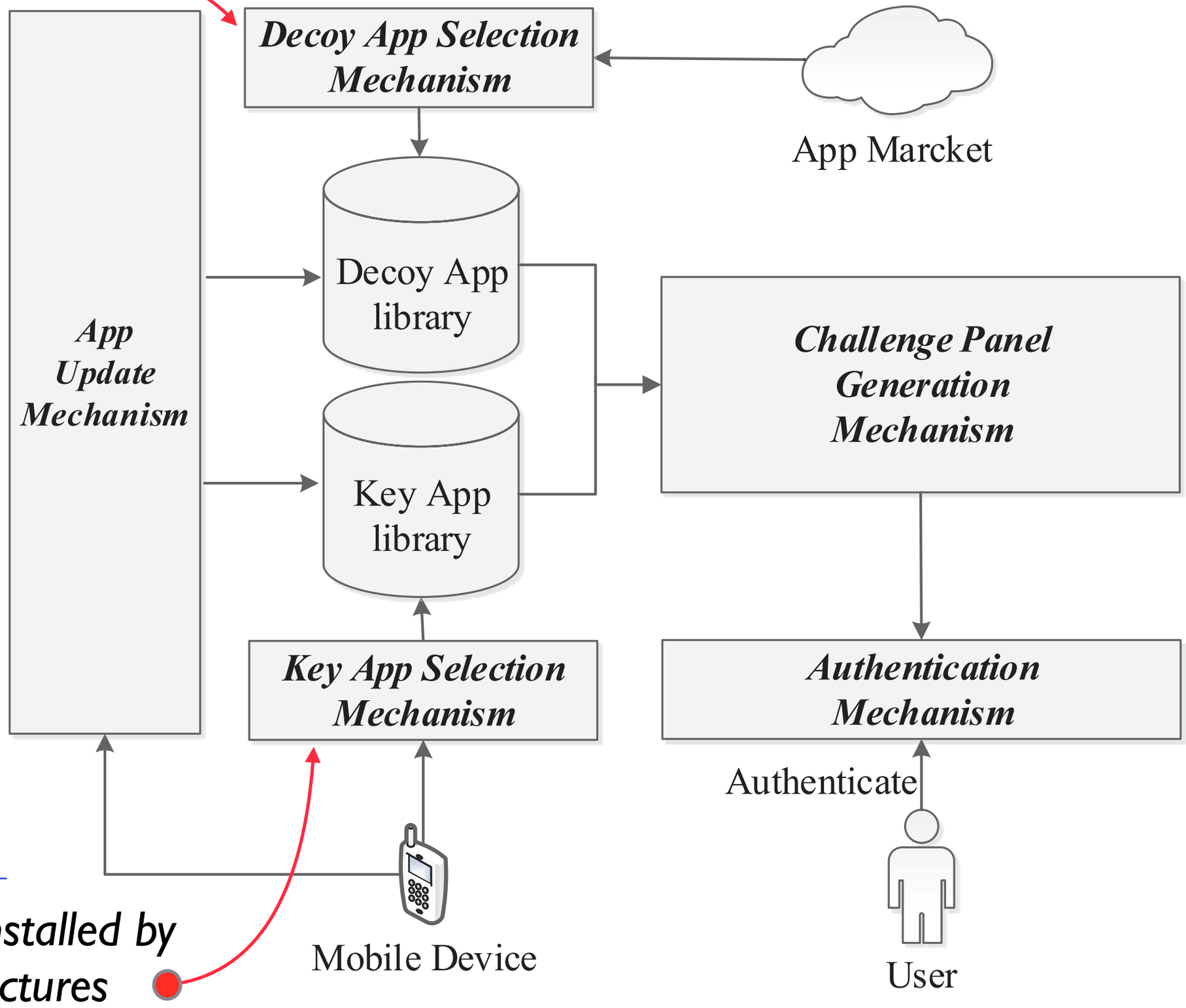
PassApp Mechanisms

key : decoy = 1:3, same category, similar rankings, etc

install a new app: *add this app to key app library, add 3 decoy apps to the decoy app library*

uninstall an app: *delete this app from key app lib and move it into a blacklist, remove corresponding decoy apps from the decoy app library.*

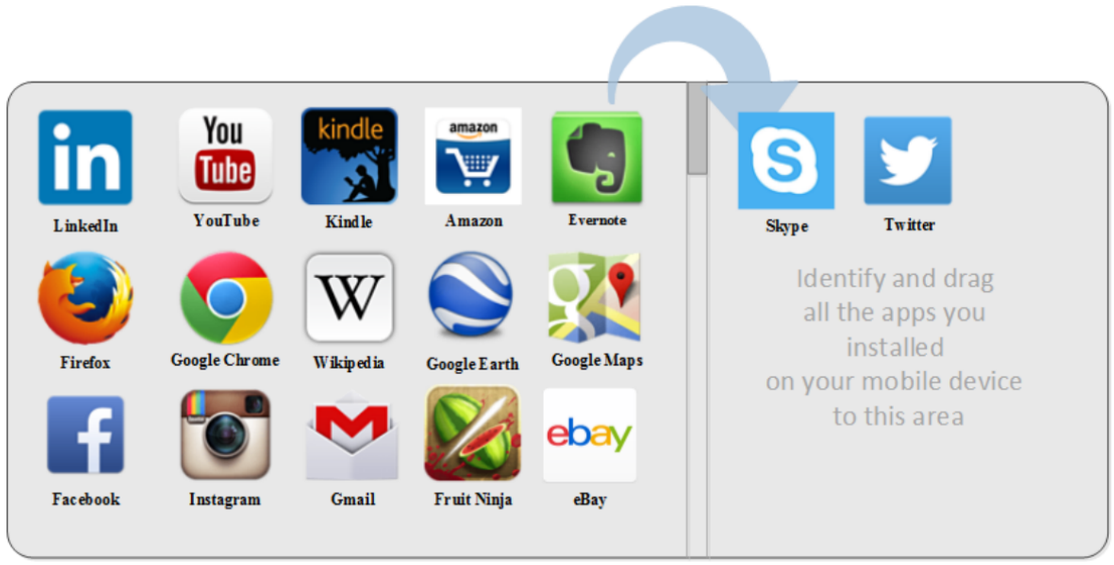
rule out the apps preinstalled by device and OS manufactures



User Study

Day 1

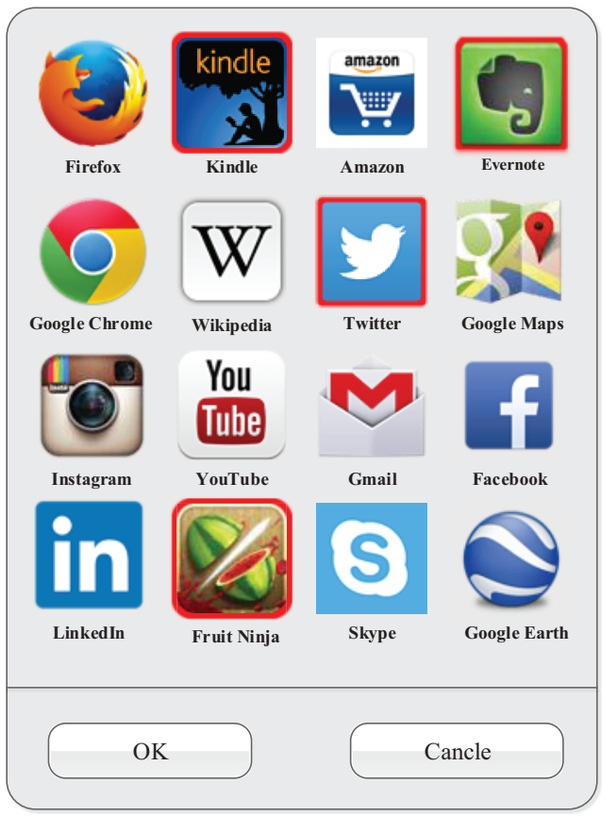
User Study 1:
How well can users correctly recognize the apps they have installed?



42 participants

Day 2

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



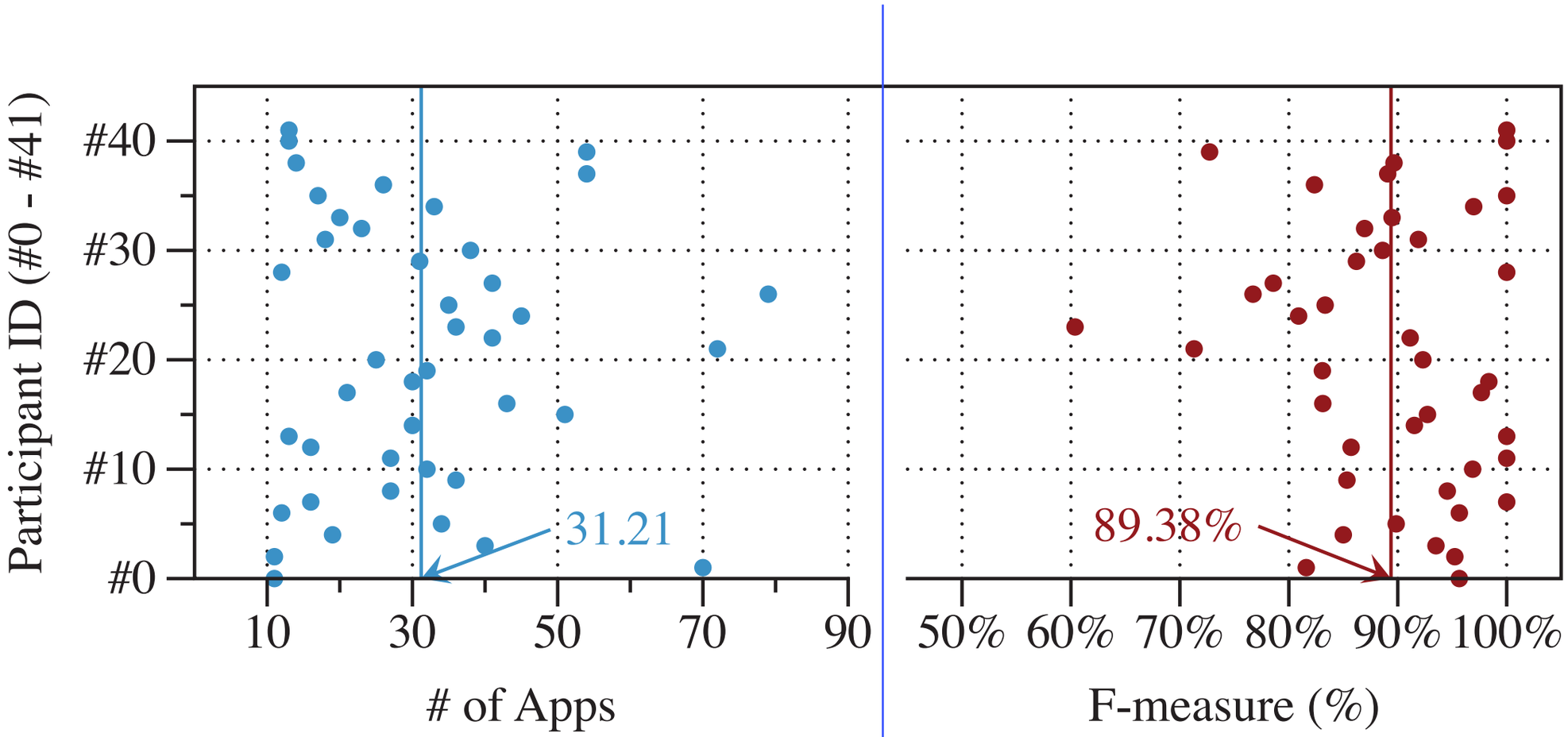
unlock 10 times

*42 *10*

Login Time

Success Rate

Memory about Installed Apps



Max:79, Min: 11, SD: 16.79

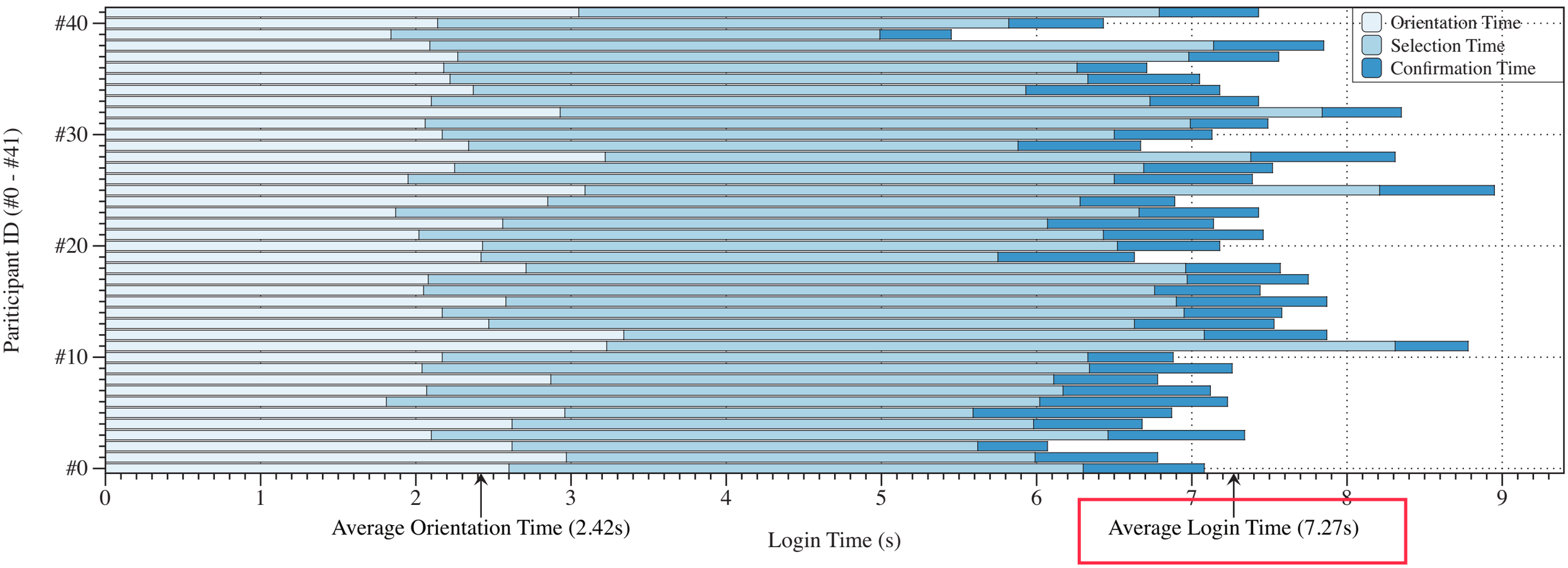
$$F_{measure} = \frac{P \times R}{P + R} \times 2$$

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

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

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 confirmation time: 0.76s

Security Analysis

Brutal-force Attacks

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

0.055%

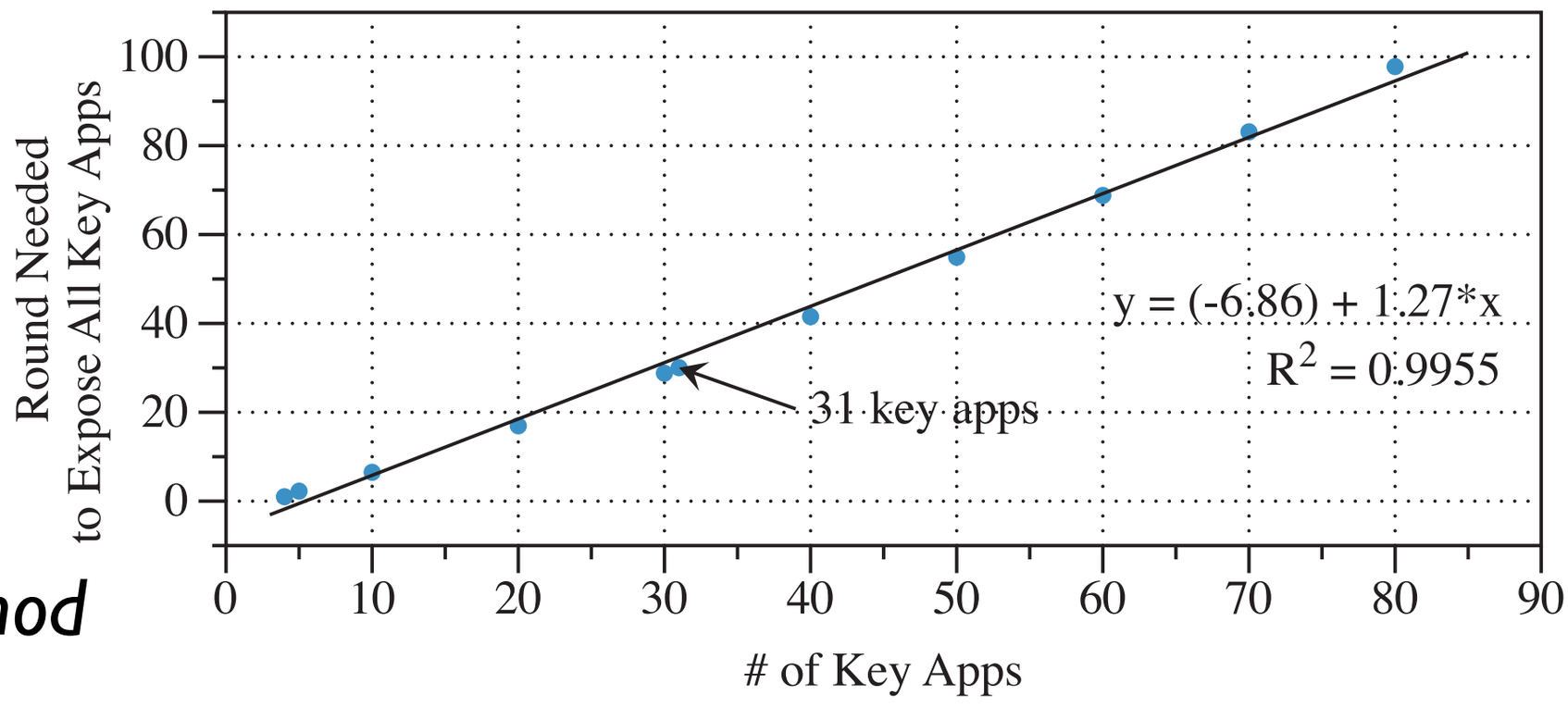
One-time shoulder Surfing Attacks

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

s = 31, E = 0.52

Multi-time shoulder Surfing Attacks

Monte Carlo Method



Session 1: Guessing Attacks

know nothing about the victims

Session 2: Acquaintance Attacks #1

Observe: 10seconds/screen; break: 3 minutes; 5 login attempts

Session 3: Acquaintance Attacks #2

Observe: 10seconds/screen; break: 3 minutes; 5 login attempts

Session 4: Acquaintance Attacks #3

Observe: 10seconds/screen; break: 3 minutes; 5 login attempts

8 victims X 10 attackers X 5 login attempts = 400 attempts (each session)

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

0.055% (theoretical)

Limitations of PassApp

- *Key app selection*
  - ✴ *popular apps, communication apps*
- *Decoy app selection*
  - ✴ *app market, device manufacture, OS, language,etc*
- *Login time (challenge)*

Conclusion

- *PassApp is the first graphical password that utilizes user's existing memory about installed apps as passwords*
  - *without a password registration stage*
  - *no extra memory burden*
- *PassApp performs better on login time and success rate than most graphical passwords*
  - *reasonable login time: 7.27s (6.51s when OK button is removed)*
  - *high success rate: >95%*
- *PassApp has sufficient security against common attacks*
  - *brute-force attacks (0.055%) and dictionary attacks (0.75%)*
  - *shoulder surfing attacks: average 30 times*
  - *acquaintance attacks: to some extent, it can withstand such attacks*

Download PassApp for Android: sunhp.org/passapp/passapp.apk

or scan the QR Code and Download

Web: sunhp.org/passapp

Email: pass_app@yahoo.com

Information Security Lab of Peking University