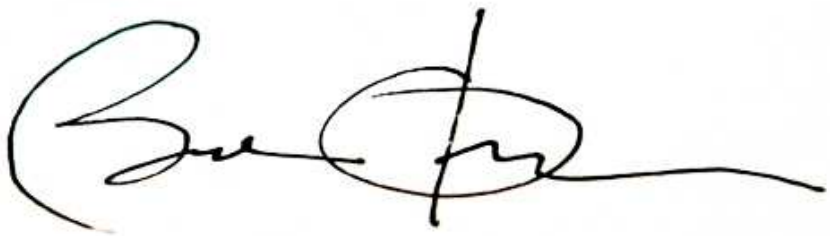
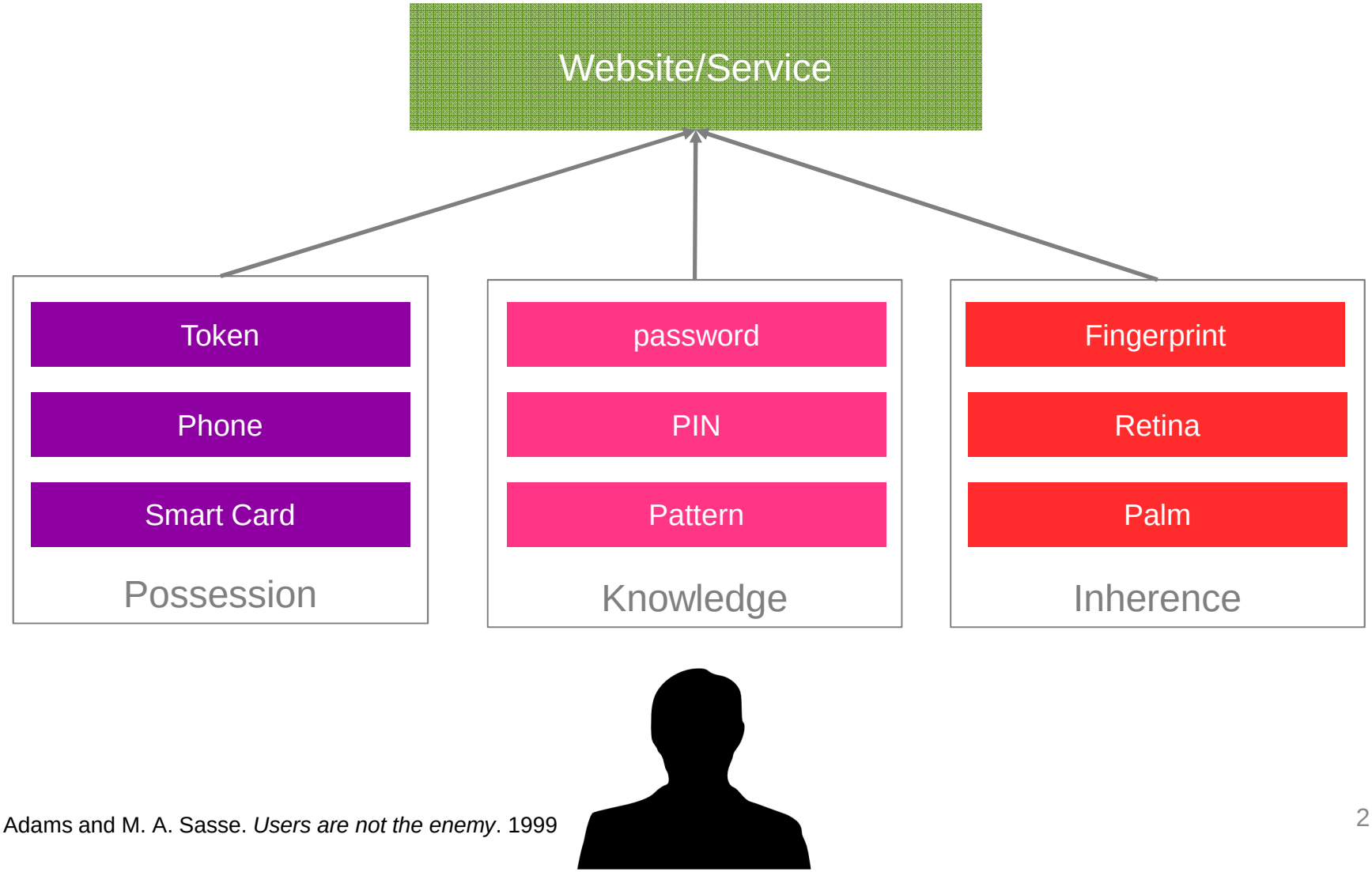


A Comparative Usability Study of Two-Factor Authentication

Emiliano de Cristofaro[1], **Honglu Du**[2], **Julien Freudiger**[2], Gregory Norcie[3]
UCL[1], PARC[2], Indiana University[3]

Two Factor (2F) Authentication



A. Adams and M. A. Sasse. *Users are not the enemy*. 1999

Two Factor vs One Factor

+

More secure

-

Less usable

Slower

Unfamiliar

N. Gunson et al. *User perceptions of security and usability of 1F and 2F in automated telephone banking*, 2011

D. D. Strouble et al. *Productivity and usability effects of using a two-factor security system*, 2009

C. S. Weir et al. *Usable security: User preferences for authentication methods in ebanking and the effects of experience*, 2010

This Presentation

Observations

Large offering of two factor solutions

Lack of metrics to measure 2F usability

Problem

Is there a difference in usability among 2F?

Contributions

Comparative usability study

Pre-study interview

Explorative quantitative study

Pre-Study Interviews

Goal

Understand popular 2F in use, context and motivations

Participant Recruitment

Mailing lists and social media (Google+ and Facebook)

Announced paid interviews for user study on authentication

Online screening survey to know more about potential participants

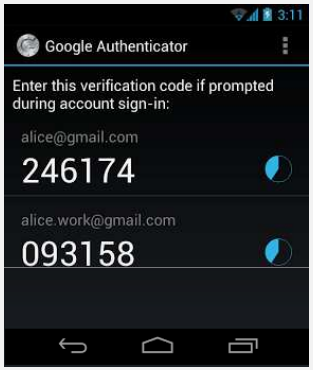
9 out of 29 mostly from Silicon Valley, familiar with 2F

Findings

Adoption

Security token

SMS or email



Smartphone app

Motivation

Forced to

Incentivized

Wanted to

“I use 2F to obtain higher limits on online banking transactions”

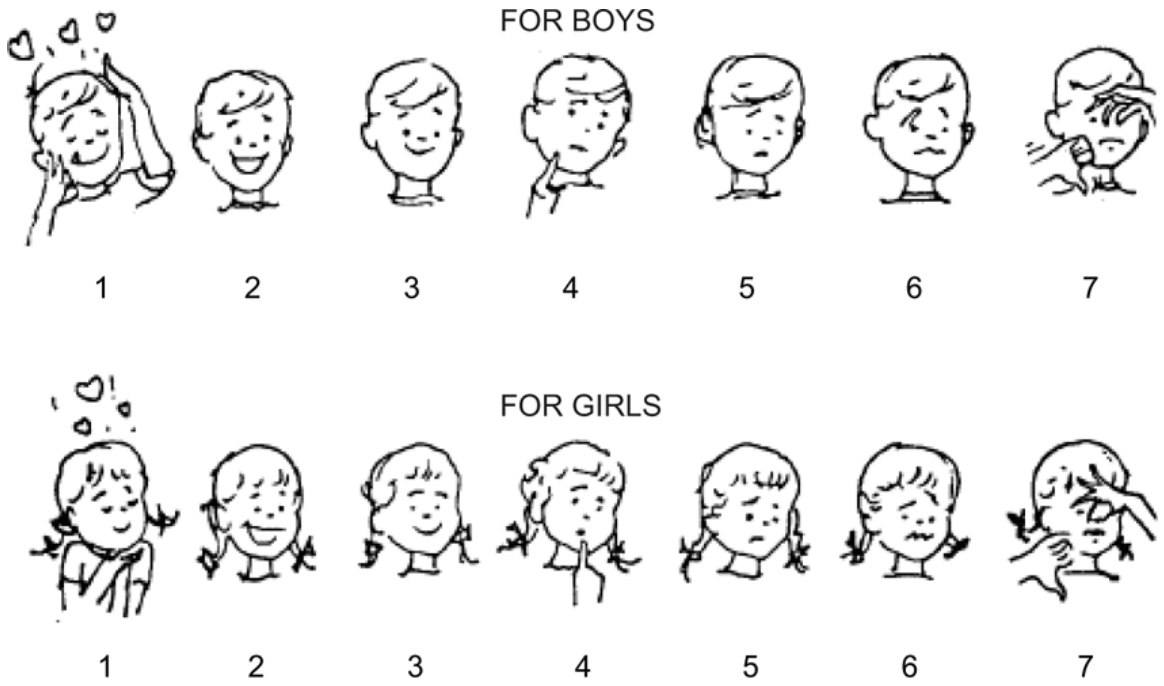
“I use 2F to avoid getting hacked”

Context

Work

Personal

Financial



QUANTITATIVE SURVEY

“An artisan must first sharpen his tools if he is to do his work well.”
Confucius

Quantitative Survey

Two main challenges

How to recruit participants?

What questions to ask?

Existing usability metrics

SUS - System Usability Scale (10 questions)

QUIS - Questionnaire for User Interface Satisfaction (27 questions)

PUEU - Perceived Usefulness and Ease of Use (12 questions)

CSUQ - Computer System Usability Questionnaire (19 questions)

…

Software focused, not for 2F technologies

Usability Questions

Quick

Helpful

Concentration

User Friendly

Not Enjoy

Stressful

Convenient

Enjoy

Reuse

Need Instruction

Secure

Frustrating

Trust

Match

Easy

J. Bonneau, etc. The quest to replace passwords: a Framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy, 2012.

A. Karole, etc. A comparative usability evaluation of traditional password managers. In ICISC, 2011.

User Distribution

Online survey

219 participants from Mechanical Turk

SUS and 15 other questions on usability

Group	2F Technologies Used	# of Participants
1	Token	11
2	Email/SMS	77
3	App	7
4	Token & Email/SMS	29
5	Token & App	3
6	Email/SMS & App	50
7	All three	41
Total		219

Results

Adoption and Context

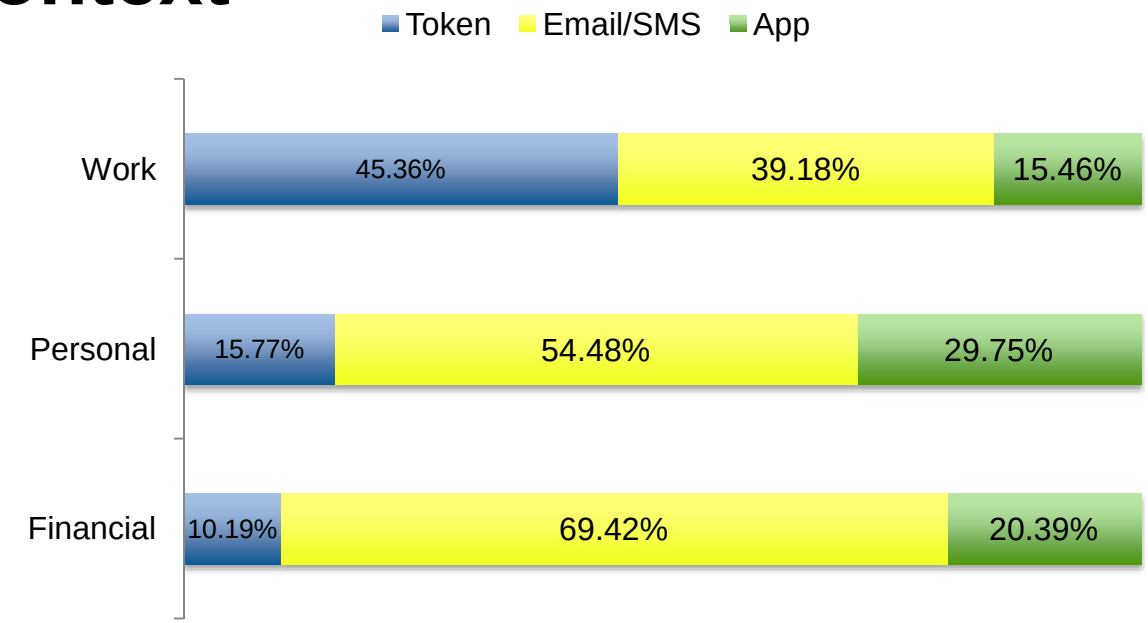
Adoption

SMS/Email is the most popular 2F (89.95%)

App (45.20%)

Token (24.20%)

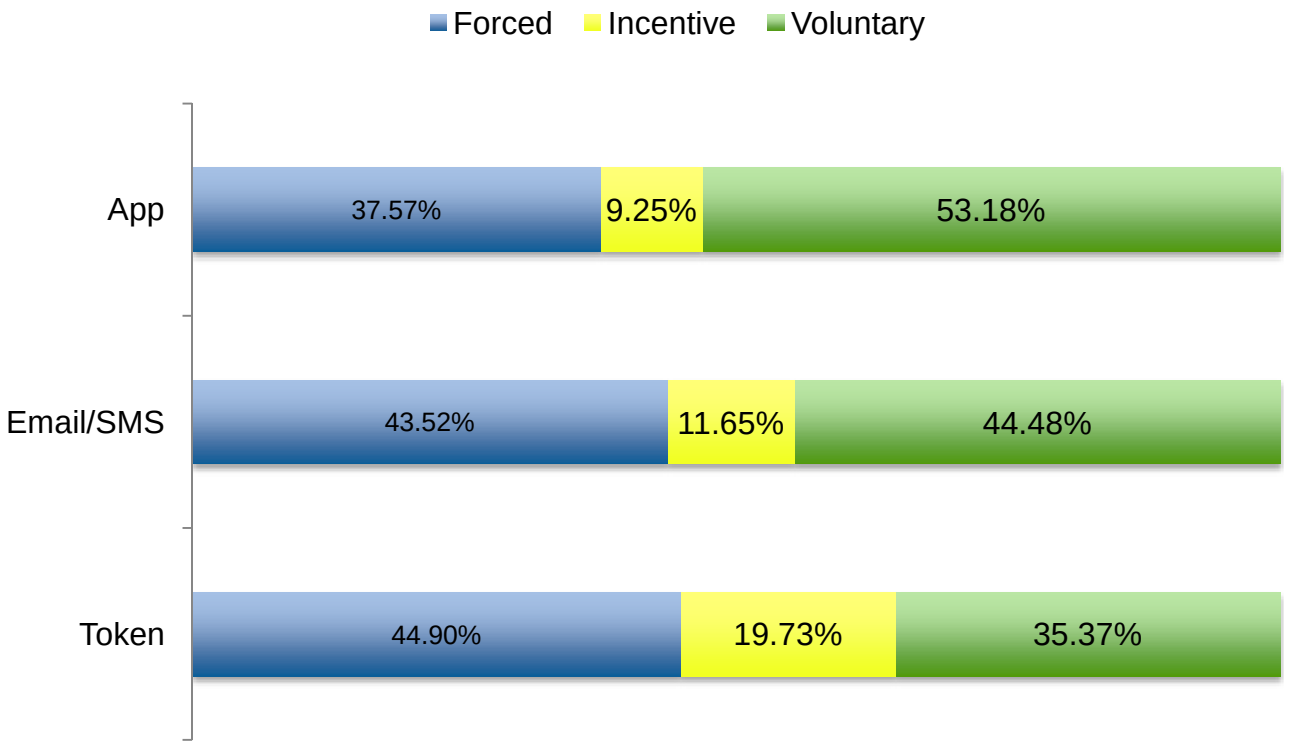
Context



$X^2(4, 582)= 65.18, p<.0001)$

Results

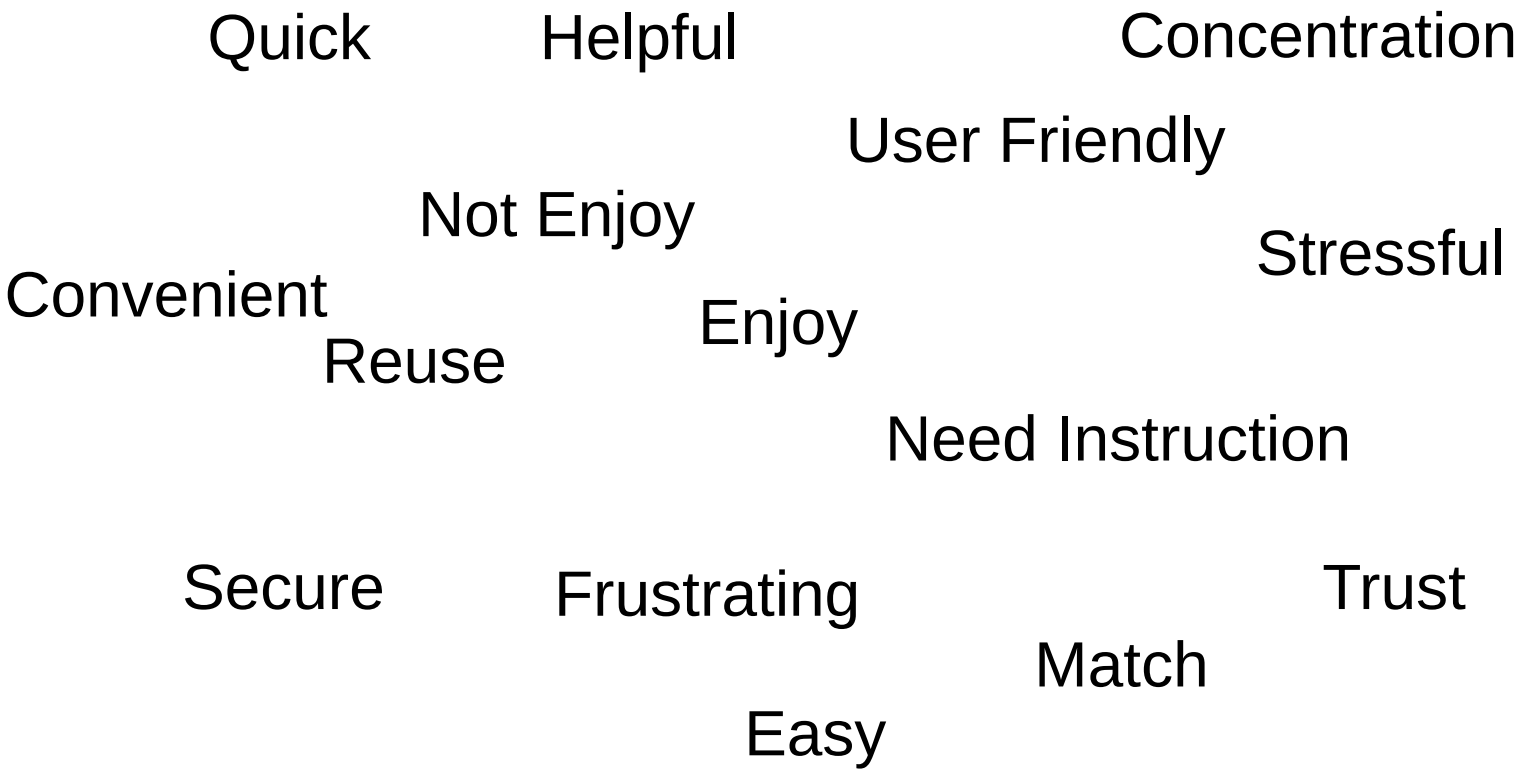
Motivations



$X^2(4, 775)= 14.68, p<.0001)$

Results

Exploratory Factor Analysis



J. Bonneau, etc. The quest to replace passwords: a Framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy, 2012.

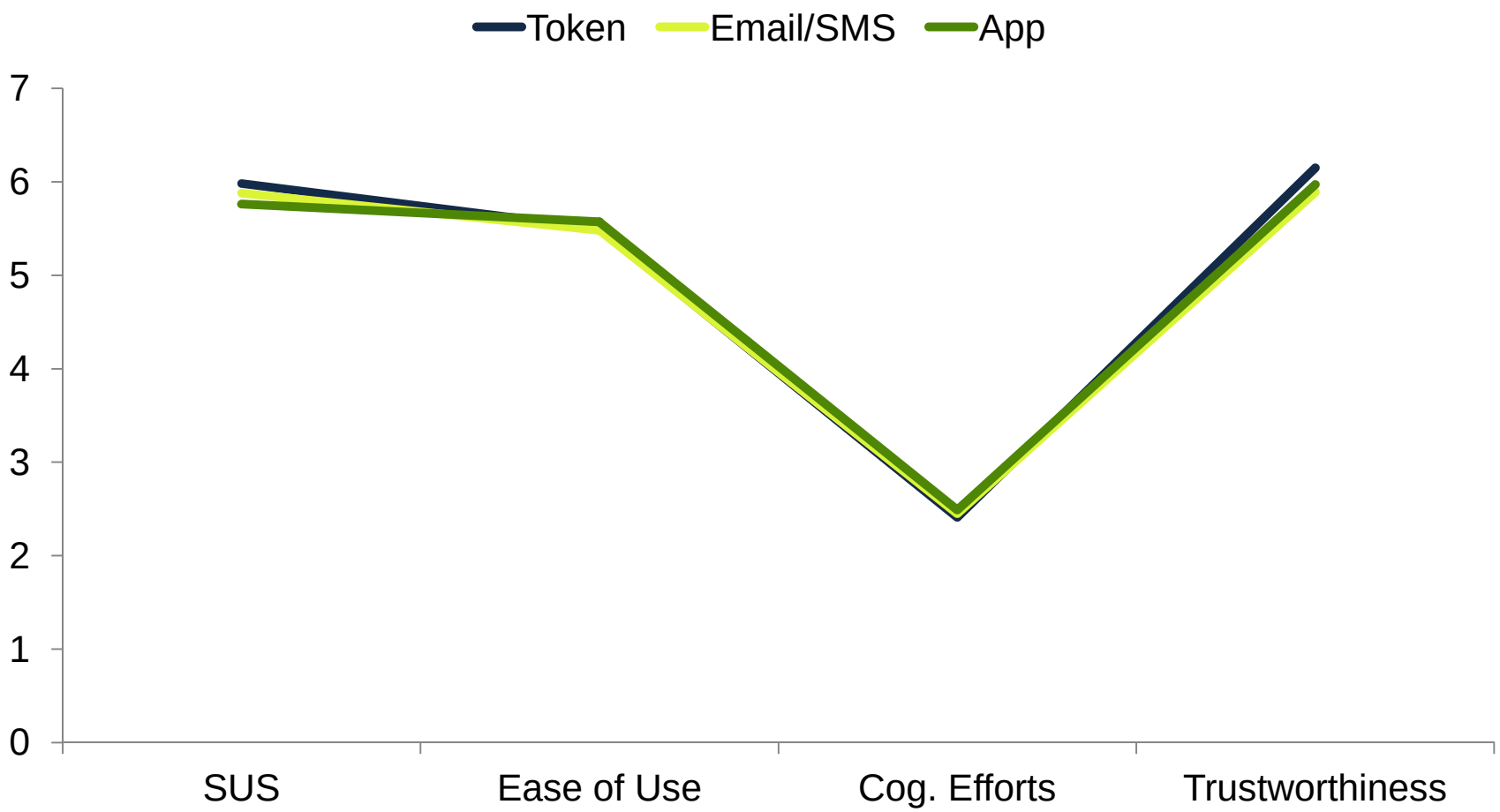
A. Karole, etc. A comparative usability evaluation of traditional password managers. In ICISC, 2011.

Results

Exploratory Factor Analysis

Ease of Use	Cognitive Efforts	Trustworthiness
Quick	Need Instruction	Trust
Convenient	Concentration	Helpful
Enjoy	Stressful	Secure
Reuse	Match	
Not Enjoy	Frustrating	
User Friendly		
32%	15%	14%
	Variance Explained	

Usability Comparison



Usability Comparison

MANOVA analysis (groups 4, 6 & 7)

DVs: Ease of use, Cognitive Efforts and Trustworthiness

IV: Technology (2F technologies used)

Covariates: Age and gender

Results

No main effect of Technology

Some usability differences w.r.t age and gender:

Email/SMS and Token users (group 4)
The elderly (Md=3) need more Cognitive Efforts than the young (Md=2, *p=0.003*)

Email/SMS and App users (group 6)
The elderly (Md=5.5) find that 2F are less trustworthy than the young (Md=6, *p=.0007*)

Users of all 3 technologies (group 7)
Females (Md=2.75) need more Cognitive Efforts than males (Md=2.0, *p=.001*)

Conclusion

Main results

Different 2F technologies are preferred in different contexts

Did not find usability difference among three 2F technologies

Identified two additional dimensions of 2F usability: *Cognitive Efforts* and *Trustworthiness*

Future work

Larger variety of 2F technologies and participants

Develop a usability scale for 2F technologies

BACKUP

Methodology

Interviews

1 on 1 meeting, $10 Amazon Gift Card compensation

Questions

1. Which 2F have you used? (Adoption)
2. How does 2F work? (Understanding)
3. Why do you use 2F? (Motivation)
4. Recall last time you used 2F? (Familiarity)
5. What issues do you have with 2F? (Comments

PIN from a paper/card
Digital certificate
RSA token code
Verisign token code
Paypal token code
Google Authenticator
PIN received by SMS/email
USB token
Smartcard

Participants' Profile

Selected 9/29 from survey

Most of them from silicon valley

Only participants familiar with 2F

Age: 21 to 49

Gender: 5 males, 4 females

Education: High school to PhD

Security: 5/9 background in computer security