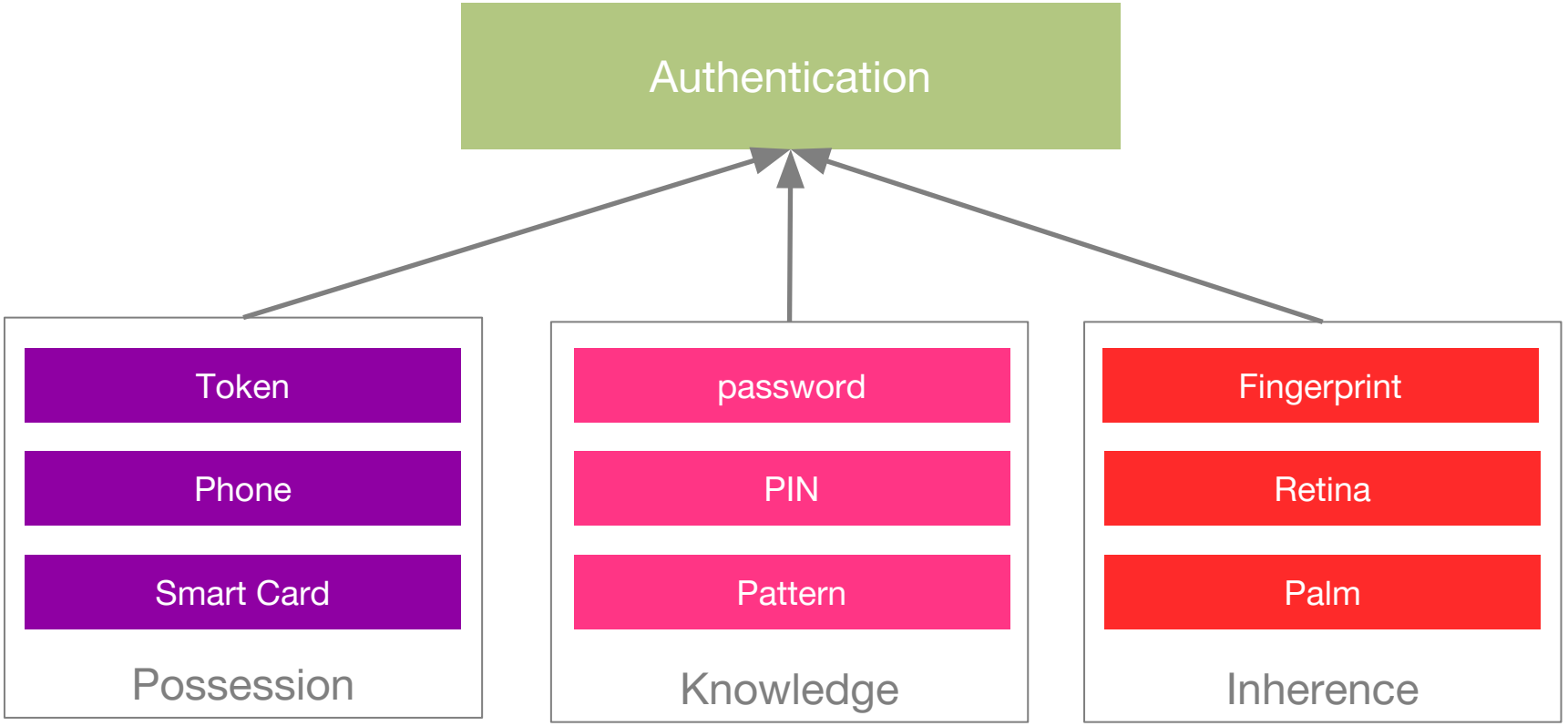
Experiences with Studying Usability of Two-Factor Authentication Technologies

Emiliano De Cristofaro
https://emilianodc.com

UCL

Two Factor (2FA) Authentication



2FA Evolution

Adoption no longer restricted to enterprise

2FA offered as an option by most numerous cloud & service providers

New players and technologies in the market (not just RSA tokens for VPN)

Why Study 2FA Usability?

Unusable authentication yields:

- More lockouts, resets → loss of productivity
- Longer auth tasks → drive customers/business away

2FA deployed in different contexts

- Different primary tasks → no one-size-fits-all tech

Prior Work: 2FA vs Passwords

+

More secure

-

Less usable

Slower

Unfamiliar

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

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

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

Our Objectives

1. (Comparatively) study users' perceptions of 2FA usability, understand motivations for adoption, context of use

2. In-depth analysis of usability issues with actual users, specific primary tasks

Two Studies

1. E. De Cristofaro, H. Du, J. Freudiger, G. Norcie.
   Two-Factor or not Two-Factor? A Comparative Usability Study of Two-Factor Authentication
   8th NDSS Workshop on Usable Security (USEC 2014)

2. K. Krol, E. Philippou, E. De Cristofaro, M. A. Sasse.
   "They brought in the horrible key ring thing" Analysing the Usability of Two-Factor Authentication in UK Online Banking
   9th NDSS Workshop on Usable Security (USEC 2015)

Hypotheses

Context of use, motivation, frequency of use significantly affect perceived usability

In online banking, even though there's only one primary task, no one-size-fits-all

Two Studies

1. E. De Cristofaro, H. Du, J. Freudiger, G. Norcie.
   Two-Factor or not Two-Factor? A Comparative Usability Study of Two-Factor Authentication
   8th NDSS Workshop on Usable Security (USEC 2014)

2. K. Krol, E. Philippou, E. De Cristofaro, M. A. Sasse.
   "They brought in the horrible key ring thing" Analysing the Usability of Two-Factor Authentication in UK Online Banking
   9th NDSS Workshop on Usable Security (USEC 2015)

Pre-Study Interviews

Goal

Understand popular 2FA 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 2FA

Participants' Profile

Selected 9/29 from pre-screening survey

Age: 21 to 49

Gender: 5 males, 4 females

Education: High school to PhD

Security: 5/9 background in computer security

Methodology

Interviews

1 on 1 meeting, $10 Amazon Gift Card compensation

Questions

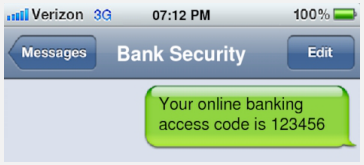
1. Which 2FA have you used? (Adoption)
2. How does 2FA work? (Understanding)
3. Why do you use 2FA? (Motivation)
4. Recall last time you used 2FA? (Familiarity)

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

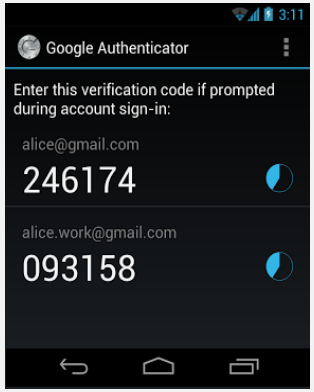
Findings

Adoption

Security token



SMS or email



Smartphone app

Motivation

Forced to

Incentivized

Wanted to

"I have to use it to work from home"

"I use 2FA to obtain higher limits on online banking transactions"

"I use 2FA to avoid getting hacked"

Context

Work

Personal

Financial

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 2FA technologies

Usability Questions (Likert)

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	2FA 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

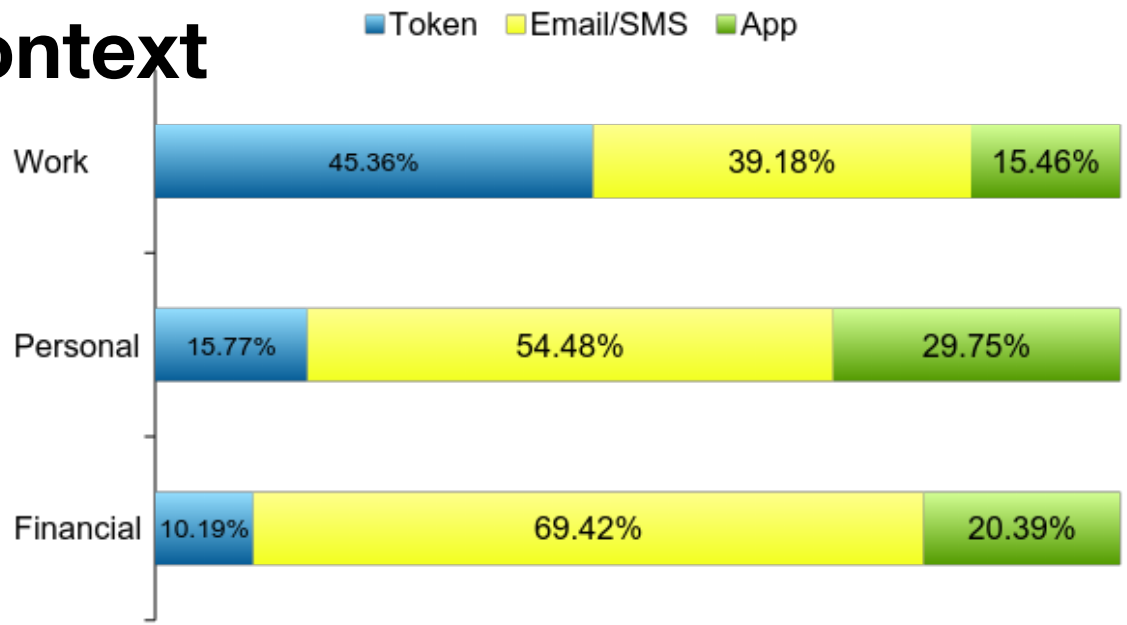
Adoption

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

App (45.20%)

Token (24.20%)

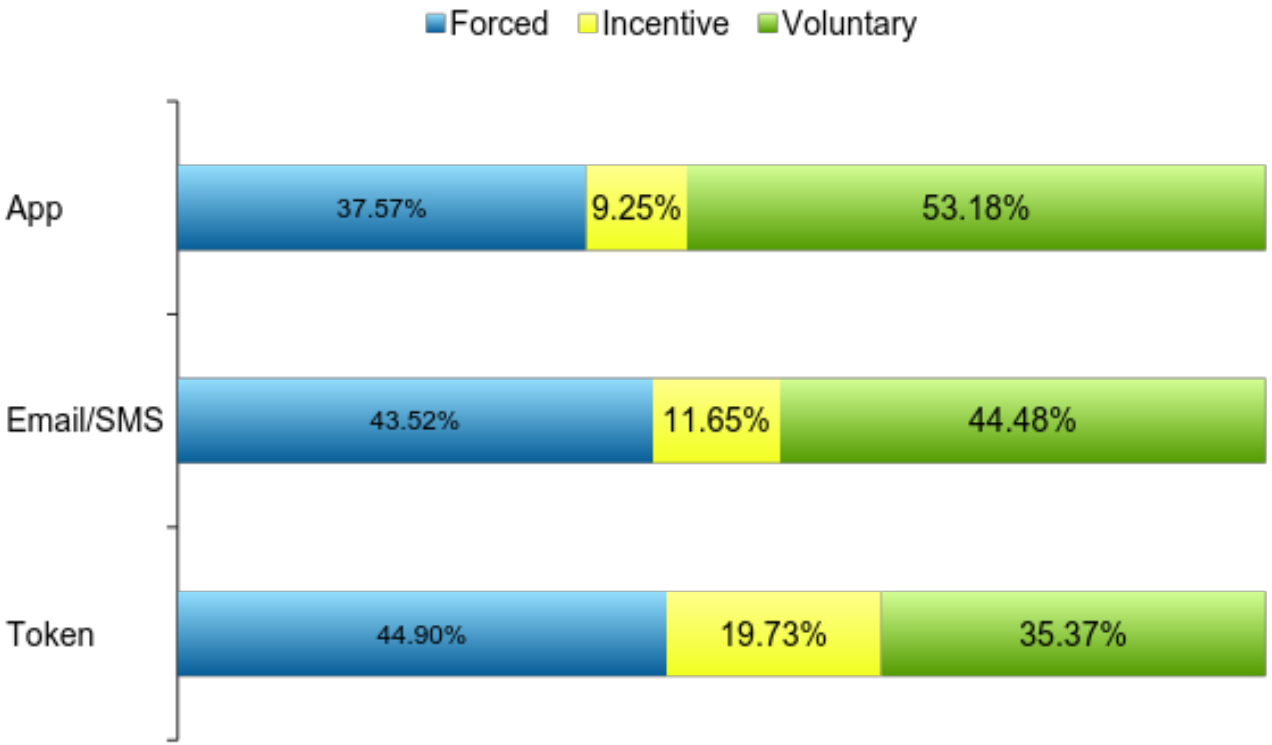
Context



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

Results

Motivations



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

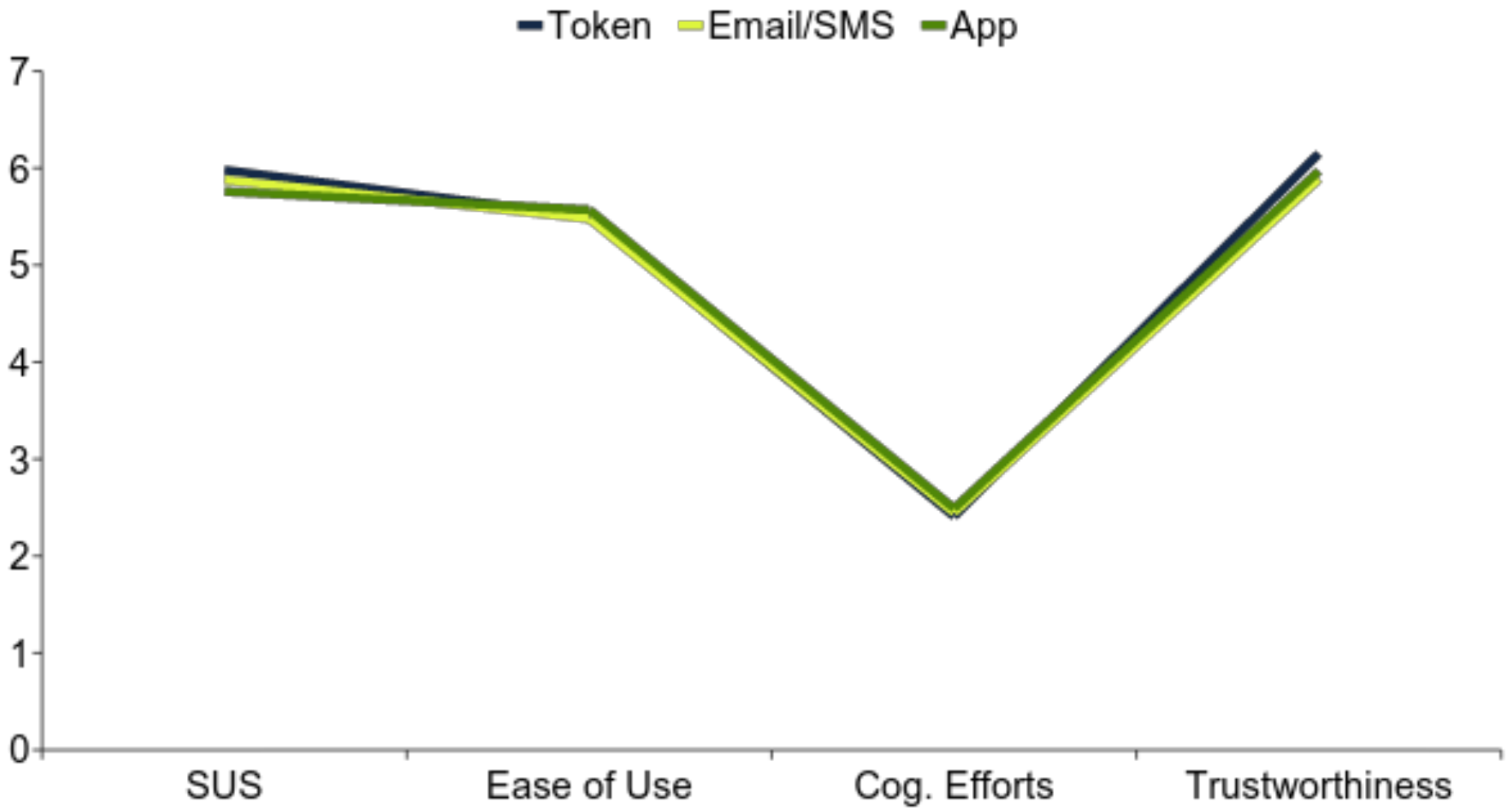
Results

Exploratory Factor Analysis

Ease of Use	Cognitive Efforts	Trustworthiness
Quick	Need Instruction	Trust
Convenient	Concentration	Helpful
Enjoy	Stressful	Secure
Reuse	Match	
Not Enjoy	Frustrating	
User Friendly		

SUS

Usability Comparison



Usability Comparison

Does context|motivation|technology impact usability?

Via MANOVA analysis

Answer...

No

Usability Comparison

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

Email/SMS and Token users (group 4)

The elderly (Md=3) need more Cognitive Efforts (Md=2, *p=0.003*)

Email/SMS and App users (group 6)

The elderly (Md=5.5) find that 2FA are less trustworthy (Md=6, *p=.0007*)

Users of all 3 technologies (group 7)

Females (Md=2.75) need more Cognitive Efforts (Md=2.0, *p=.001*)

Hypotheses

Context of use, motivation, frequency of use significantly affect perceived usability

→ Somewhat negative result

In online banking, even though there's only one primary task, no one-size-fits-all

Two Studies

1. E. De Cristofaro, H. Du, J. Freudiger, G. Norcie.
   Two-Factor or not Two-Factor? A Comparative Usability Study of Two-Factor Authentication
   8th NDSS Workshop on Usable Security (USEC 2014)

2. K. Krol, E. Philippou, E. De Cristofaro, M. A. Sasse.
   "They brought in the horrible key ring thing" Analysing the Usability of Two-Factor Authentication in UK Online Banking
   9th NDSS Workshop on Usable Security (USEC 2015)

2FA landscape in the UK

Hardware tokens: Card Reader, SecureKey

SMS

Phone call

Mobile phone app

Participants

66 people filled in a pre-screen, 21 were chosen

11F / 10M, age range: 19-69

(mean: 32.4, SD=10.87)

2FA technologies used:

- Card Reader: 16
- SecureKey: 9
- OTP via SMS: 5
- OTP over the phone: 4
- OTP via smartphone app: 3

Study stages

1. Preliminary interviews (~30mins/£5)

2. Diary (10-12 days)

3. Final interviews (~30mins/£15)

Interview results: Hardware tokens

Advantages

Easy to use (4)

Portable (4)

Easy to incorporate into everyday life (4)

Disadvantages

Needs to remember to bring it (7)

Inconvenient (5)

Frustrating to use (4)

Irritating (3)

"It's OK when I am at home, but when you are at work and you are pretending you are actually doing work when you are actually checking on your account, then you have to bring out this calculator thing and it's kind of obvious you are not doing work. I'd rather have something where I am just on the screen and it's lot quicker." (P11)

Authentication terminology

"*Is it a passphrase or passcode or key phrase what they need? [chuckling] I think it is slightly confusing. Although I'm experienced [...], it's frustrating*." (P08)

Interruption to the primary task

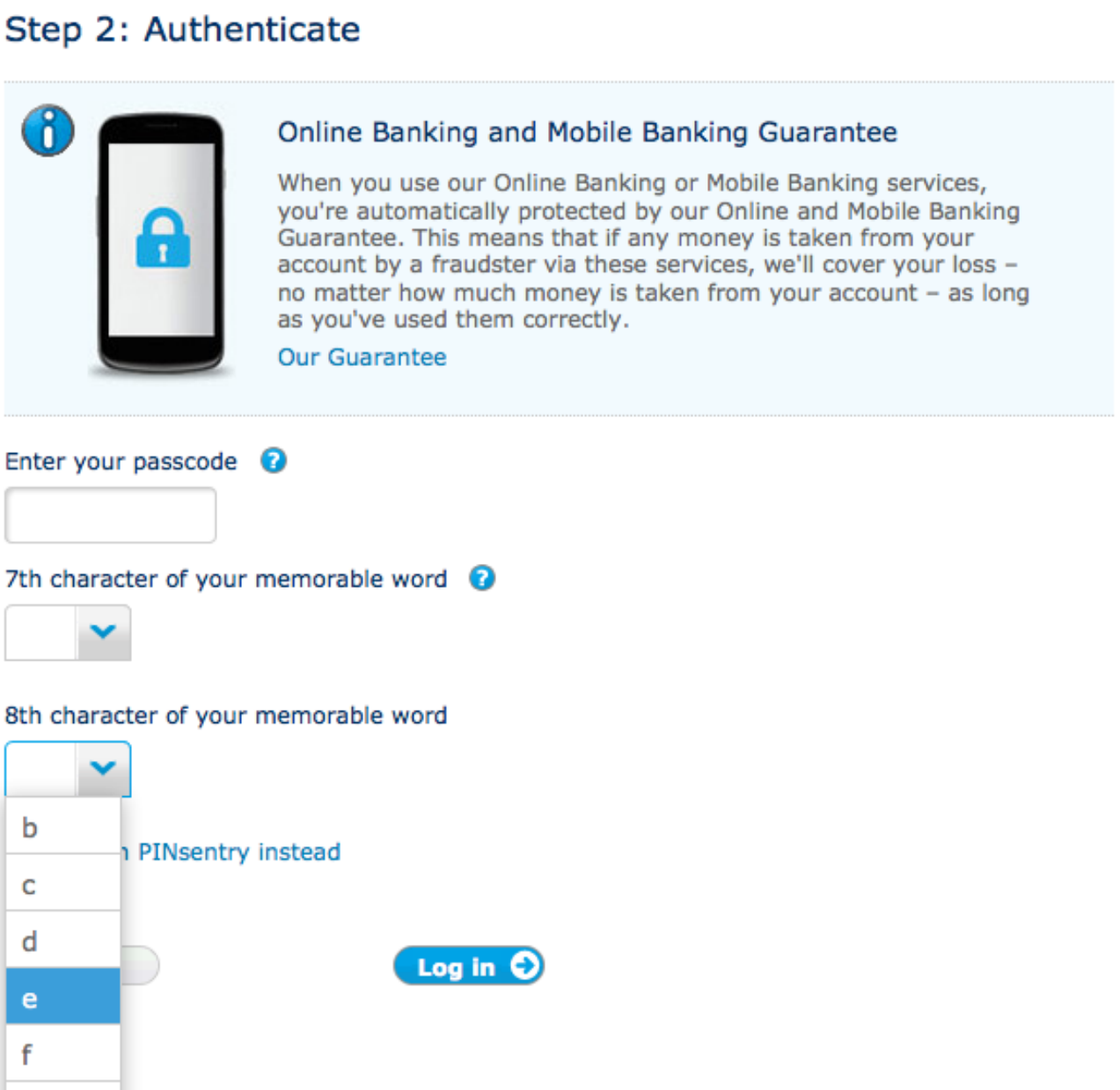
"*If I am in a rush, I maybe misspell my surname or I do not enter the card number correctly […] I'll have to get myself together mentally and let's say "Focus! Whatever is in your mind, forget it.*" (P14)

Other problems

Assigned usernames prevented participants from logging in

Cumbersome resets led to simpler credentials

Use of drop-down menus



Mental models

Credentials are checked manually by bank employees

Where do OTPs come from?

Card reader needs protection, information can be stolen off it

Security rituals reassure users (e.g., anti-virus, hiding the token, using password as memorable answer)

Ideal authentication

Biometrics!

“I think, in a few 100 years from now you’ll just put your finger on a machine and it reads your fingerprint. Today, it’s slow – you know fast is good! The faster the better.”

Implicit authentication

Reliability concerns (5)

Privacy concerns (6)

"*I could see implicit working but you'll probably run to privacy issues about that: Who's doing the software? How's the monitoring done? Who gets the information from the monitoring? blah blah blah. That would be the real issue.*" (P10)

Diary results

17 participants kept an authentication diary for approx. 11 days

90 entries, 5.29 per person (1-15, SD=3.99)

There were problems on 12 occasions (13.3%)

- Mistyped credentials (5)
- Misplaced tokens (2)
- Wrong memorable answer, wrong sequence of steps, forgotten username

Participant satisfaction

Lower when they generated an OTP to authenticate

Lower the more pieces of information they had to enter

Lower with banks that required a token to generate an OTP

Recommendations

Give customers choice of authentication options

Unify wording for credential names

Check your security features actually work

- Use of drop-down menus
- Providing selected characters out of order

Next steps...

Threat modeling

Economic aspects

Behavioral biometrics as 2nd factor

Contextual security and 2FA

Thanks to…

Honglu Du

Julien Freudiger

Kat Krol

Eleni Philippou

M. Angela Sasse

Victoria Bellotti