Two Heads are Better Than One: Security and Usability of Device Associations in Group Scenarios

Ronald Kainda, Ivan Flechais, and A.W. Roscoe

Oxford University Computing Laboratory, UK

14 - 16 July, 2010

Outline

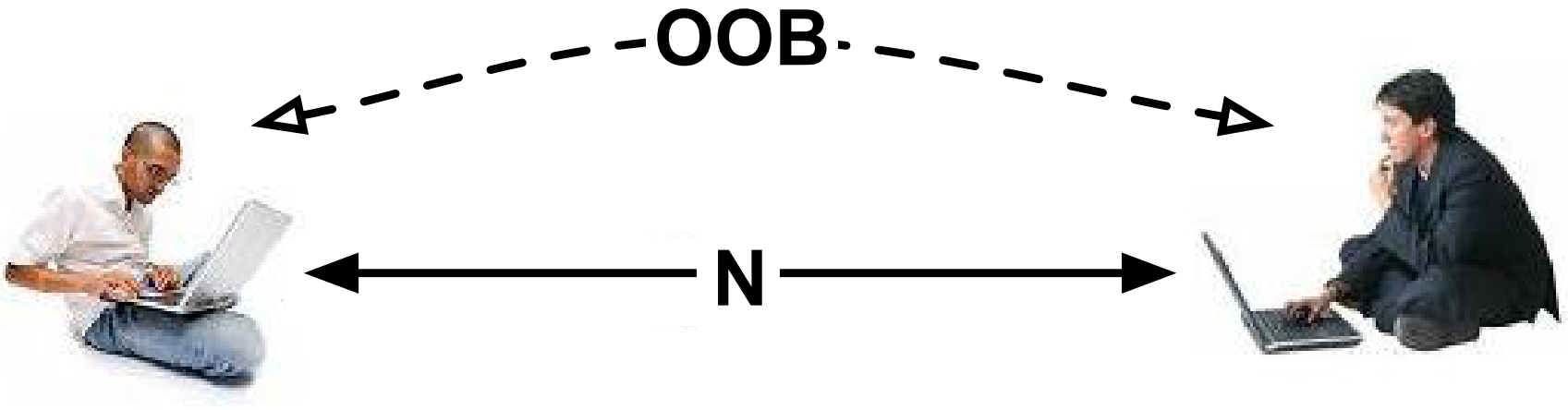
1. Introduction
2. Experimental Design
3. Results
4. Analysis and Discussion
5. Summary and conclusion

Outline

1. Introduction
2. Experimental Design
3. Results
4. Analysis and Discussion
5. Summary and conclusion

Introduction - Device association

Human-Interactive Security Protocols (HISP)



- OOB = Out-Of-Band, N = Normal

Introduction - Device association

Single user scenarios

- Two or more devices
- User has control of all devices
- Data available on performance of methods

Introduction - Device association

Group scenarios

- Different challenges from single user scenario
- Different context
- No studies

Introduction - Group device association

Association scenarios

- One-to-many
- Many-to-one
- Partial symmetric
- Full symmetric

Introduction - Group device association

Usability and security challenges

- Communication from initiator to group members
- Communication from group members to initiator
- Inattentiveness by initiator
- Inattentiveness by group members

Outline

1 Introduction

2 Experimental Design

3 Results

4 Analysis and Discussion

5 Summary and conclusion

Experimental Design

Methods – compare and confirm

- Numeric
- Images

Experimental Design

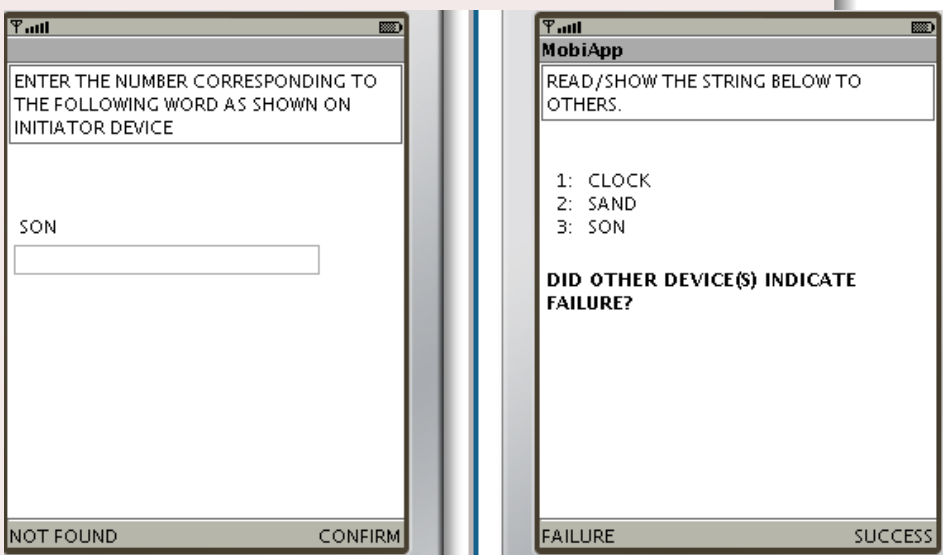
Methods – copy and enter

- Similar to Bluetooth PIN entry
- Display and keypad
- Numeric

Experimental Design

Methods – word-matching and number-typing

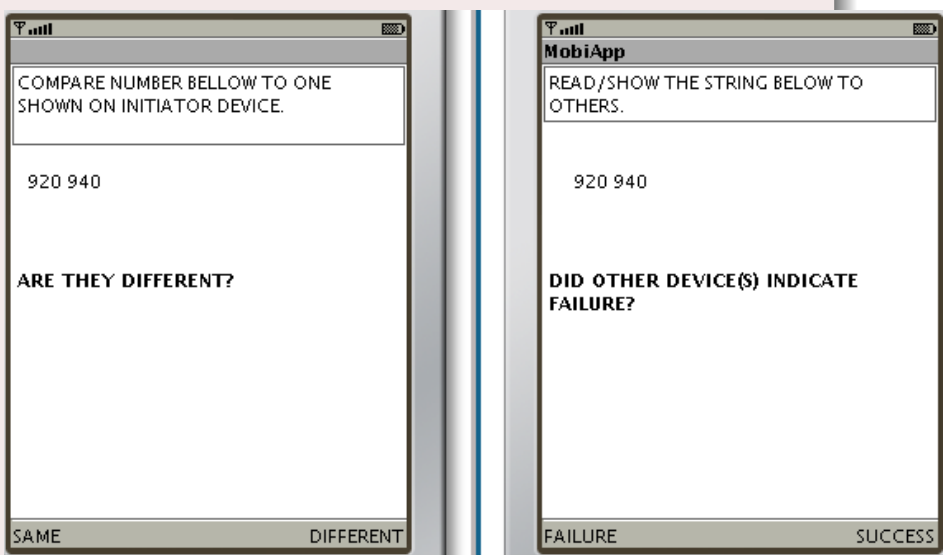
- Locally stored dictionary
  - proposed two 1024 word dictionaries
  - Phonetically distant
  - less than 40kb file
- Display and button



Experimental Design

Methods – repeated comparison

- Similar to *compare and confirm*
- Display and button
- Correct response is in 2^n



Experimental Design

Cases

- Normal case
- Failure case

Experimental Design

Design

Dependent variables

- Completion times
- Non-security failures
- Security failures

Independent variable

- Method

Experimental Design

Participants

- 47 participants

Gender	Male:	46.7%
	Female:	53.3%
Age	18 - 25	51.1%
	26 - 35	21.3%
	36 - 45	17%
	46 - 55	8.5%
	56+	2.1%
Education	High School:	19.1%
	College:	31.9%
	Graduate:	27.7%
	Postgraduate:	21.3%

Experimental Design

Participant tasks

- Primary tasks - exchanging contacts, digital cash transfer, group messaging, and group quiz
- Questionnaires
- Interview

Experimental Design - Apparatus

- Devices: Nokia N95 and Blackberry Bold 9500
  - Bluetooth support
  - Multi-tap and qwerty keyboard
- Software:
  - Simulated primary tasks
  - Device communication using Bluetooth
  - Software created a log of participant's actions
- Video camera
- Questionnaires
  - Enrolment
  - After scenario (ASQ)
  - After experiment/exit (AE)

Experimental Design

Hypotheses

- H1: there is no difference between different age groups in terms of completion times
- H2: there is no difference between different methods in terms of completion times
- H3: there is no difference between different methods in terms of rating scores

Outline

1 Introduction

2 Experimental Design

3 Results

4 Analysis and Discussion

5 Summary and conclusion

Results - Analysis by age

	ASQ (Mode)		Failures (%)		Time (Seconds)	
	Y	O	Y	O	Y	O
Compare and confirm	7(8)	6(5)	0	0	7	8
Repeated comparison	6(9)	6(3)	9	14	14	19
Copy and enter	7(9)	7(5)	5	0	12	13
Word-matching and number-typing	6(5)	6(3)	3	11	18	26

- Performance by age: Y = younger group (<36 years, n=27), O = older group (>35 years, n=9). X(Y): X = mode, Y = frequency

Statistical analysis

- *Compare and confirm* – p (2-tailed)= .666
- *Repeated comparison* – p (2-tailed) = .185
- *Copy and enter* – p (2-tailed) = .414
- *Word-matching and number-typing* – p (2-tailed) = .024.

Results - Analysis by method

Security and non-security failures

	Security %	Non-security %
Compare and confirm	0	0
Repeated comparison	2.4	17.9
Copy and enter	0	3.6
Word-matching and number-typing	0	8.3

Results - Analysis by method

Completion times

- Group members

	Min	Max	Mean
Compare and confirm	2	42	7.89
Repeated comparison	3	64	17.63
Copy and enter	5	46	12.97
Word-matching and number-typing	6	94	22.89

- Analysis of variance $F(2.084,216.77) = 36.6$ and $p = .000$
- Pairwise comparison p-values ranging from .000 to .017

- Initiators

	Min	Max	Mean
Compare and confirm	7	278	40.97
Repeated comparison	11	105	33.94
Copy and enter	8	107	36.27
Word-matching and number-typing	11	147	48.27

- Analysis of variance $F(2.04,71.3) = 1.22$ and $p = .277$

Results - Analysis by method

Rating scores - group members

- ASQ scores significant – Friedman test $\chi^2(3) = 11.655$ and p = .009
- *Copy and enter* ranked first, then *compare and confirm*, *word-matching and number-typing*, and finally *repeated comparison*
- No significance on overall scores – Friedman test $\chi^2(3) = 5.526$ and p = .137

Results - Analysis by method

Rating scores - group members

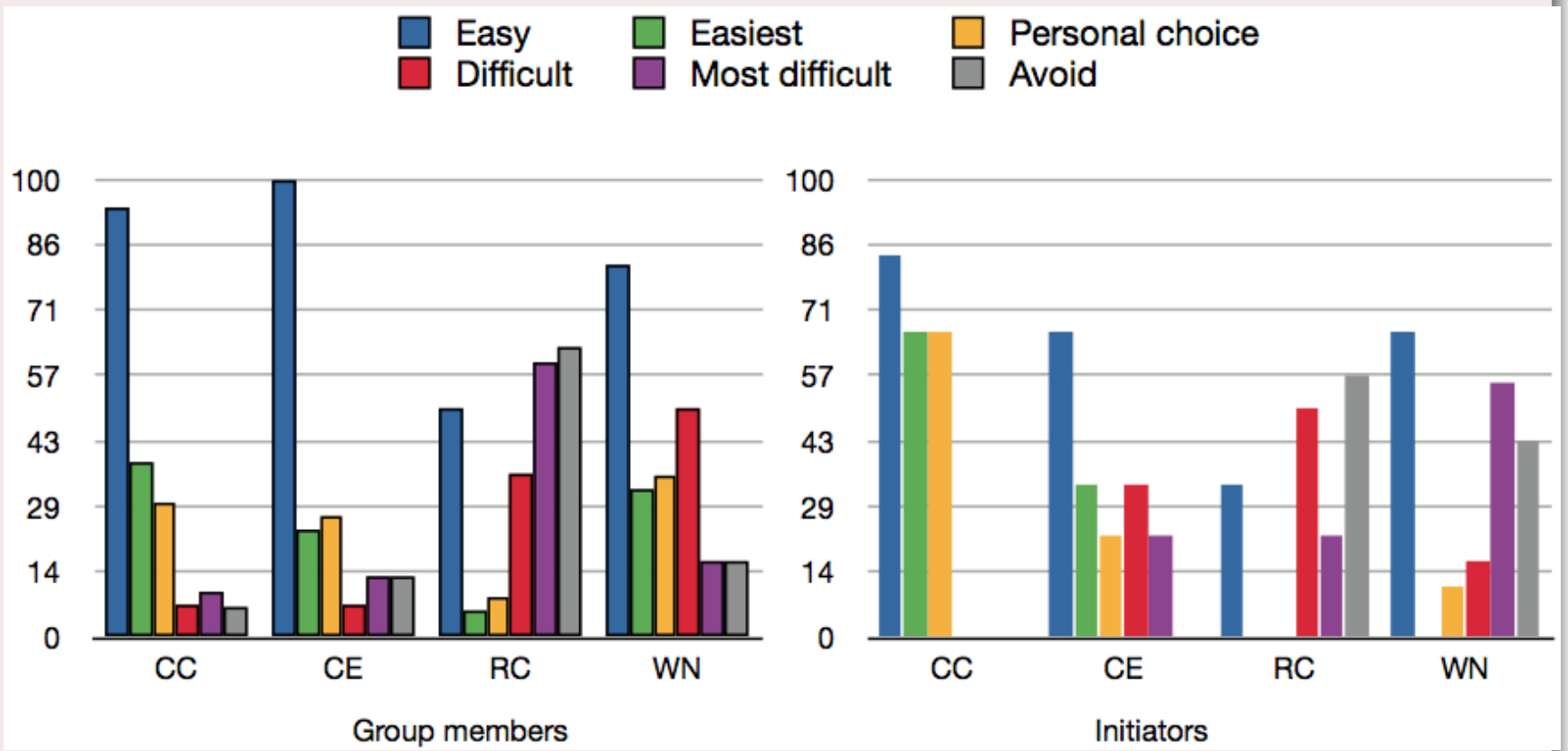
- ASQ scores significant – Friedman test $\chi^2(3) = 11.655$ and p = .009
- *Copy and enter* ranked first, then *compare and confirm*, *word-matching and number-typing*, and finally *repeated comparison*
- No significance on overall scores – Friedman test $\chi^2(3) = 5.526$ and p = .137

Rating scores - Initiators

- No significance on ASQ scores – Friedman test $\chi^2(3)$=4.558, p = .207
- Significance on overall scores – Friedman test $\chi^2(3)$=11.082, p = .011
- *Copy and enter* ranked first, followed by *repeated comparison*, *word-matching and number-typing*, and lastly *compare and confirm*

Results - Analysis by method

Preferences



Outline

1 Introduction

2 Experimental Design

3 Results

4 Analysis and Discussion

5 Summary and conclusion

Analysis and Discussion

Findings - Number 1

- Security through trial and error

Analysis and Discussion

Findings - Number 2

- Importance of context

Analysis and Discussion

Findings - Number 3

- Sum-of-efforts security

Analysis and Discussion

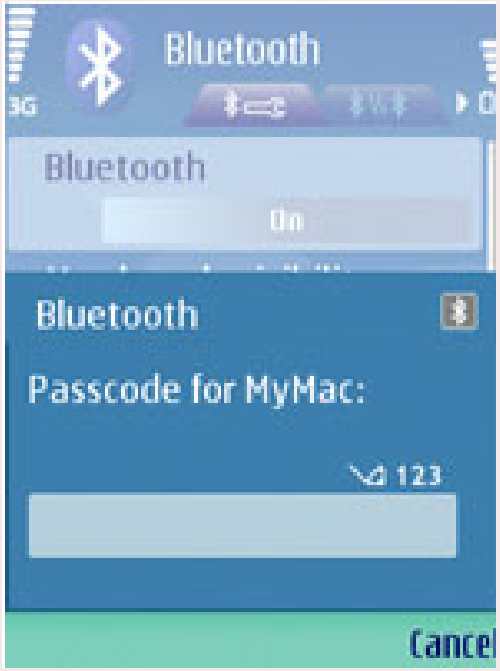
Findings - Number 4

- Insecurity of conformity

Analysis and Discussion

Findings - Number 5

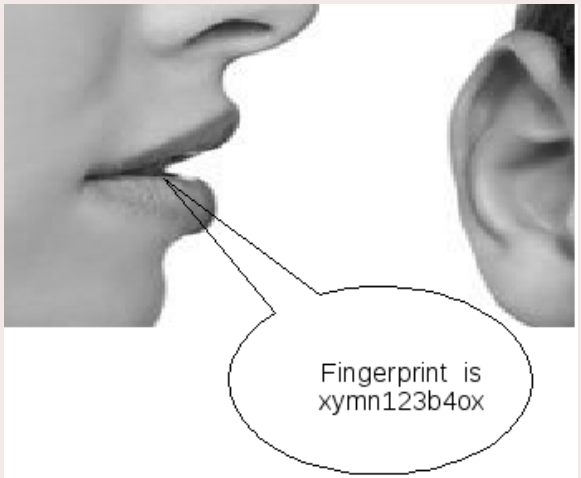
- Security beyond user interfaces



Analysis and Discussion

Findings - Number 6

- Difficult task implies security



Outline

1 Introduction

2 Experimental Design

3 Results

4 Analysis and Discussion

5 Summary and conclusion

Conclusion

- Security is a sum of efforts
- Users learn by trial and error
- Security = difficult-to-use
- Completion times depend on initiator
- Statistical significance between methods (group members completion times)
- No statistical significance between methods (initiator completion times)


THANK YOU