# Usability and Security of Out-Of-Band Channels in Secure Device Pairing Protocols

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

Oxford University Computing Laboratory

SOUPS Conference

15-17 July, 2009

# Outline

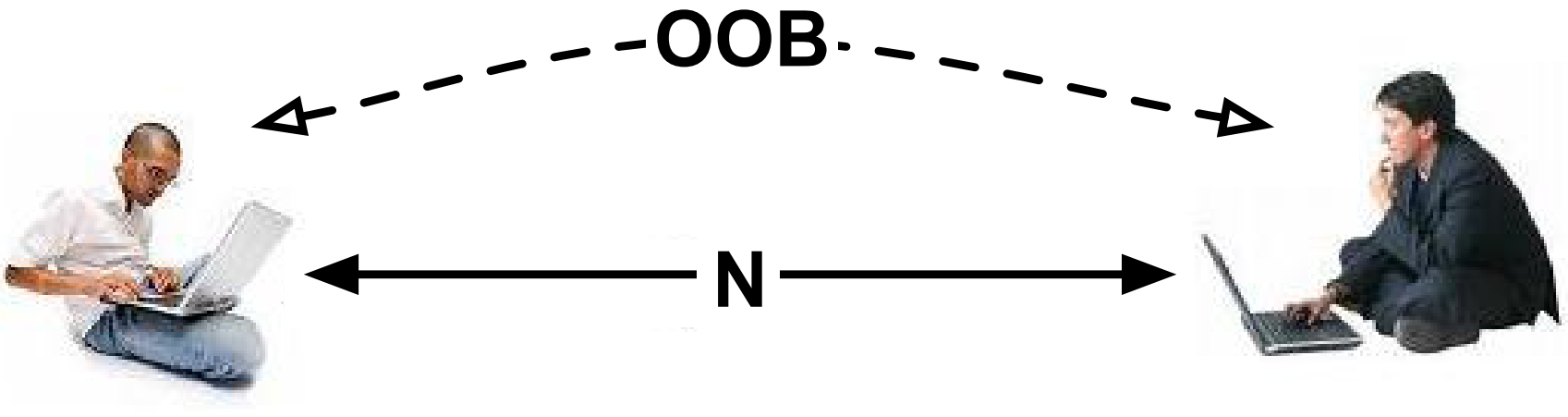
# Outline

# Introduction - Device Pairing

## Scenario

# Introduction - Device Pairing

## Human-Interactive Security Protocols (HISPs)



# Introduction - HISPs

## Security in HISPs

### Technical security

- Security based on formal proofs
- Depends on the size of the digest/fingerprint
- $b$-bits for most protocols

# Introduction - HISPs
## Security in HISPs

### Technical security

- Security based on formal proofs
- Depends on the size of the digest/fingerprint
- $b$-bits for most protocols

### Effective security

- Secure systems are socio-technical (Sasse et al.)
- Security of a protocol may depend on human effort
- Humans forget, make mistakes
- These mistakes may result in security failures
- Human failures are not covered by formal proofs
- Increasing technical security (value of $b$) may reduce effective security

# Introduction - Research Question

- Are proposed OOB methods usably secure to guarantee specified technical security?

# Outline

# HISPs - Proposed OOB Methods

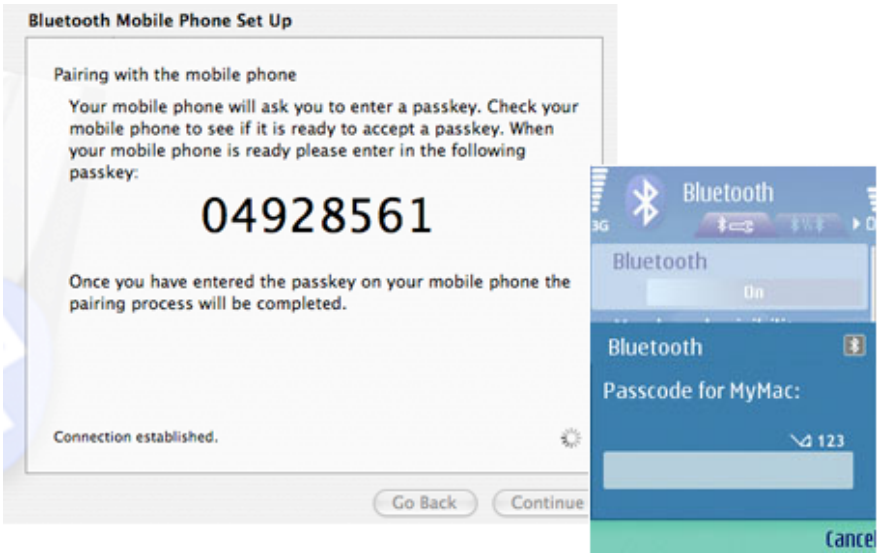
## Manual comparison

- Devices generate fingerprints
- Fingerprints displayed in appropriate format
- Users compare fingerprints and indicate on the device a match or lack of it
- Devices require display and some form of input method

# HISPs - Proposed OOB Methods

## Manual copying and entering

- One device displays a fingerprint
- User copies and types the fingerprint into one or more devices
- Requires display and keypad
- Efficiency of entry depends on affordances of devices involved



# HISPs - Proposed OOB Methods

## Auxiliary devices

- Rely on secondary devices to transfer/compare information
- Proposed devices include
  - camera phone
  - external storage devices
  - data cable etc
- May require users to carry extra hardware

# HISPs - Proposed OOB Methods

## Short-range wireless channels

- Rely on short range wireless channels
- Require devices to be no more than a few centimetres apart
- Proposed methods include:
  - infra-red
  - light
  - distance bounding[1]
- Most methods lack human verification

[1] can also use normal channel

# HISPs - Proposed OOB Methods

**Timing methods**

- Rely on transmission of information in well timed intervals
- Users coordinate the synchronisation
- Examples include
  - shaking devices (Saxena et al.)
  - pressing a button in response to some stimulus

# Outline

# Experimental Design - Methods

## DEFINITIONS

**Method**

– refers to a specific mode of comparing/transferring information between devices by humans

**Representation**

– refers to specific format in which information is presented to users

**Method-representation**

– refers to a combination of a method and representation

# Experimental Design - Method-representations

**Compare & confirm**

- Numeric
- Alphanumeric
- Words
- Sentences
- Country names
- Numeric & Sound
- Alphanumeric & Sound
- Melodies
- Images

# Experimental Design - Method-representations

**Compare & select**

- Numeric
- Alphanumeric

**Copy & enter**

- Numeric
- Alphanumeric

**Barcode**

# Experimental Design - Design

**Dependent variables**

1. Time
2. Number of non-security failures
3. Number of security failures

**Independent variable**

1. Method-representation

# Experimental Design - Participants

- 30 participants were recruited via online advertisement

| | |
|---|---|
| Gender | Male: 47%<br>Female: 53% |
| Age | 18 - 25 40%<br>26 - 35 27%<br>36 - 45 13%<br>46 - 55 3%<br>56 - 65 13%<br>66 - 75 4% |
| Education | High School: 27%<br>College: 27%<br>Graduate: 26%<br>Postgraduate: 20% |

# Experimental Design - Apparatus

- Devices: Nokia N95 and N73
  - Nokia devices are common
  - Bluetooth enabled
- Software:
  - P2P payment system
  - Device communication using Bluetooth
  - Software created a log of participant's actions
- Digital voice recorder
  - To record interviews
- Questionnaires
  - Enrolment
  - After scenario (AS)
  - After experiment/exit (AE)
- Written instructions

# Experimental Design - Procedure: Tasks

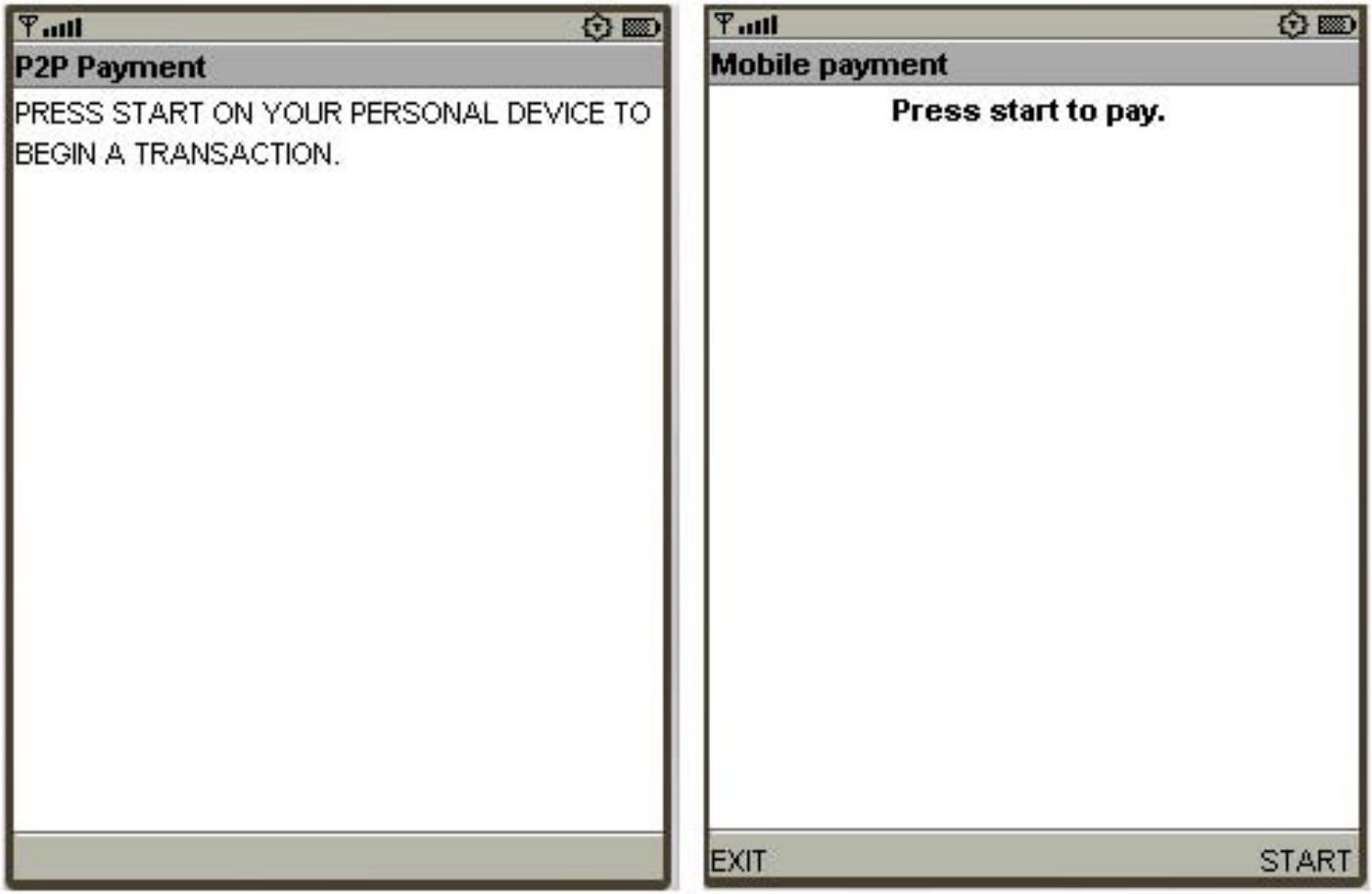



Figure: Step 1

# Experimental Design - Procedure: Tasks

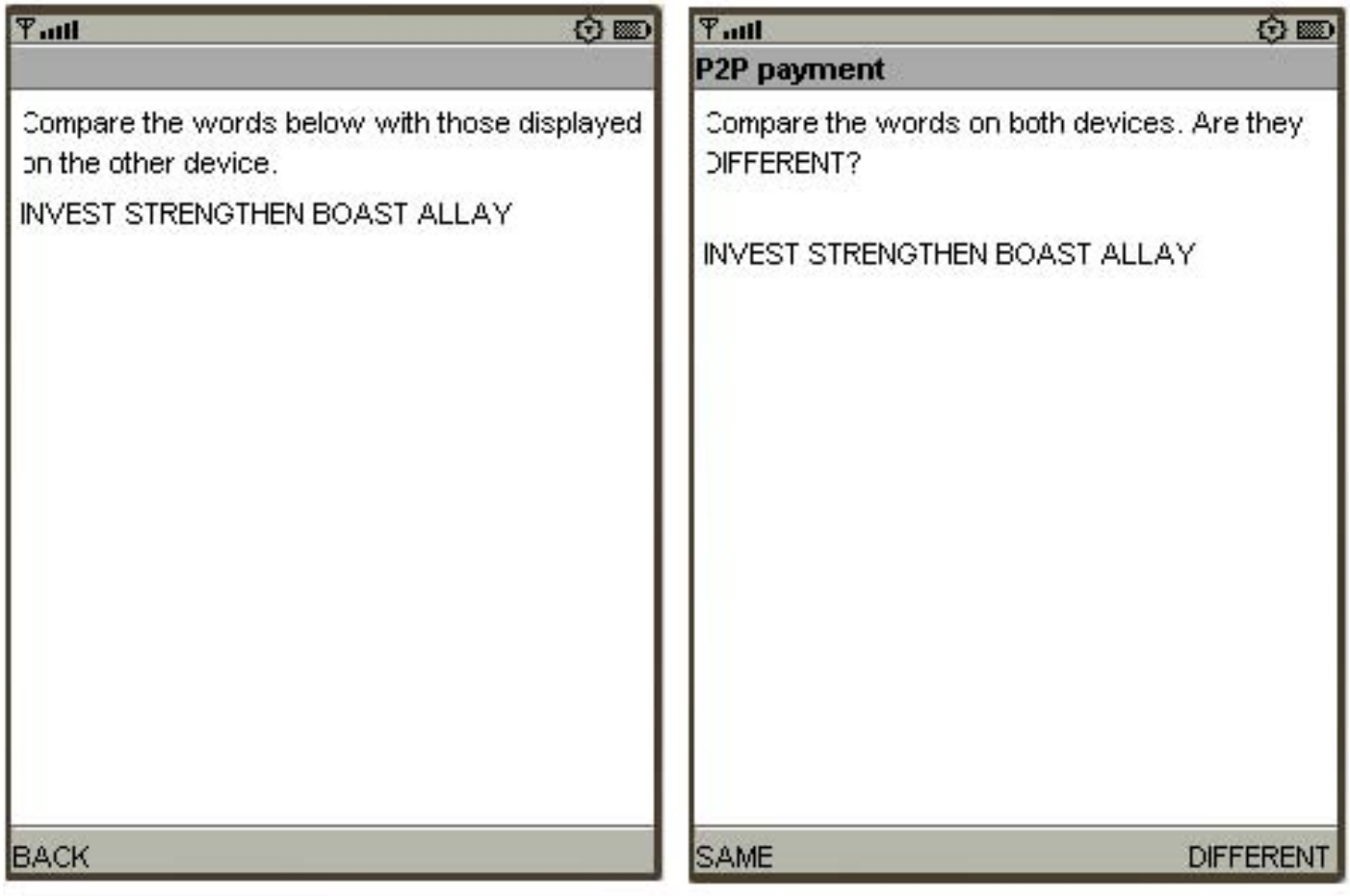



Figure: Step 2

# Experimental Design–Procedure: Tasks

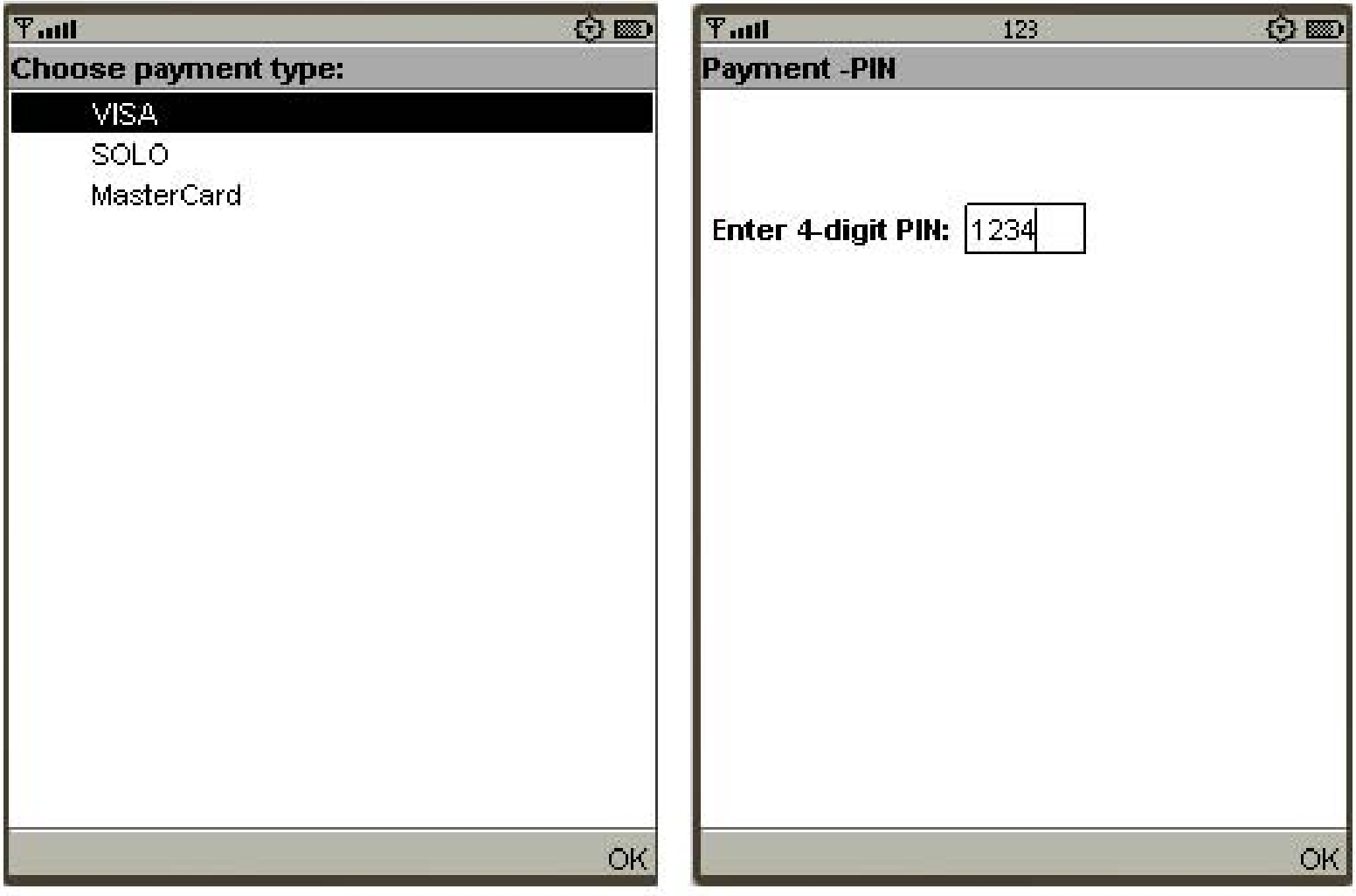



Figure: Step 3 and 4

# Experimental Design - Procedure: Tasks


Figure: Step 5 and 6

# Outline

# Results - Compare & confirm: Errors and completion times

| | Time (s) | Security failures | Non-security failures |
|---|---|---|---|
| | Mean | % | % |
| Numeric | 6 | 0 | 3.3 |
| Alphanumeric | 6 | 13.3 | 16.7 |
| Words | 7 | 3.3 | 16.7 |
| Images | 8 | 0 | 3.3 |
| Country/ City names | 9 | 0 | 3.3 |
| Sentences | 11 | 0 | 16.7 |
| Alphanumeric & sound | 12 | 3.3 | 20 |
| Numeric & sound | 14 | 3.3 | 0 |
| Melodies | 24 | 6.7 | 36.7 |

Between-subjects: $p = 0.0007$ Within-subjects - time: $p = .0000$

# Results - Compare & select: Errors and completion times

| | Time | Security failures | Non-security failures |
|---|---|---|---|
| | Seconds | % | % |
| Numeric | 9 | 10 | 10 |
| Alphanumeric | 9 | 20 | 30 |

Between-subjects: $p = 0.0000$

Within-subjects - time: $p = 0.9255$

# Results - Copy & enter: Errors and completion times

| | Time | Non-security failures |
|---|---|---|
| | Seconds | % |
| Numeric | 17 | 13 |
| Alphanumeric | 40 | 23 |

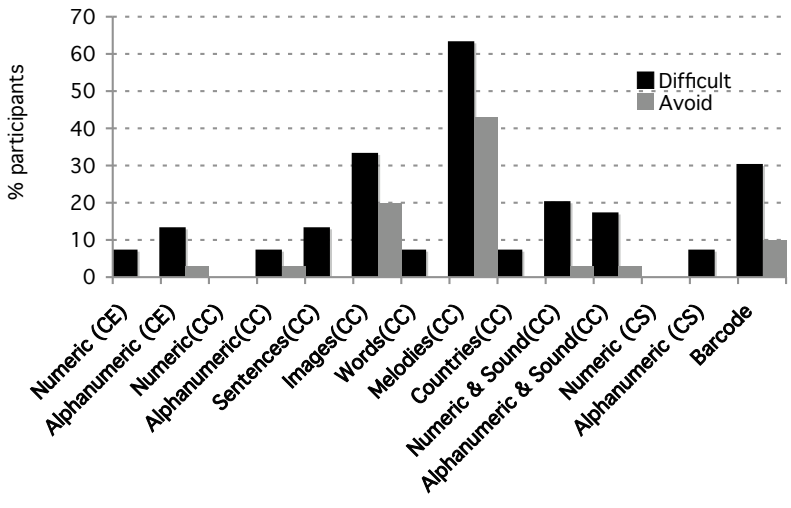
Between-subjects: $p = .7531$

Within-subjects - time: $p = .0004$

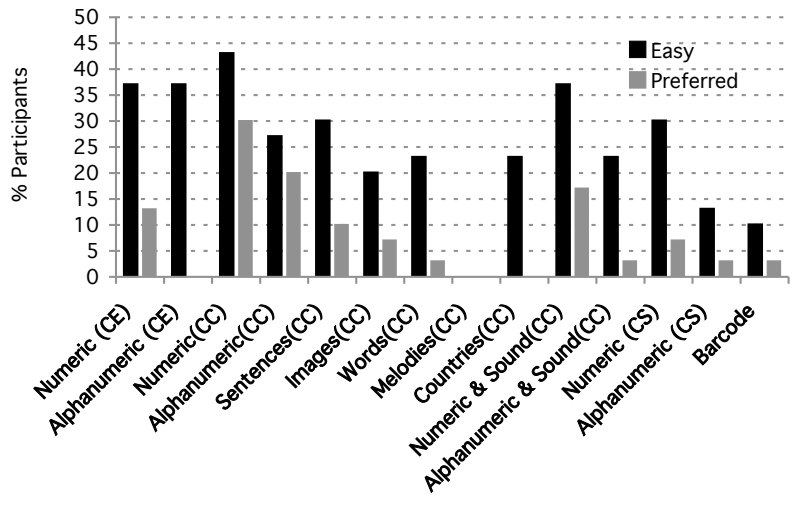
# Results - Barcode: Errors and completion times

| Time Seconds | Non-security failures % |
|---|---|
| 37 | 53 |

# Results - Preferences



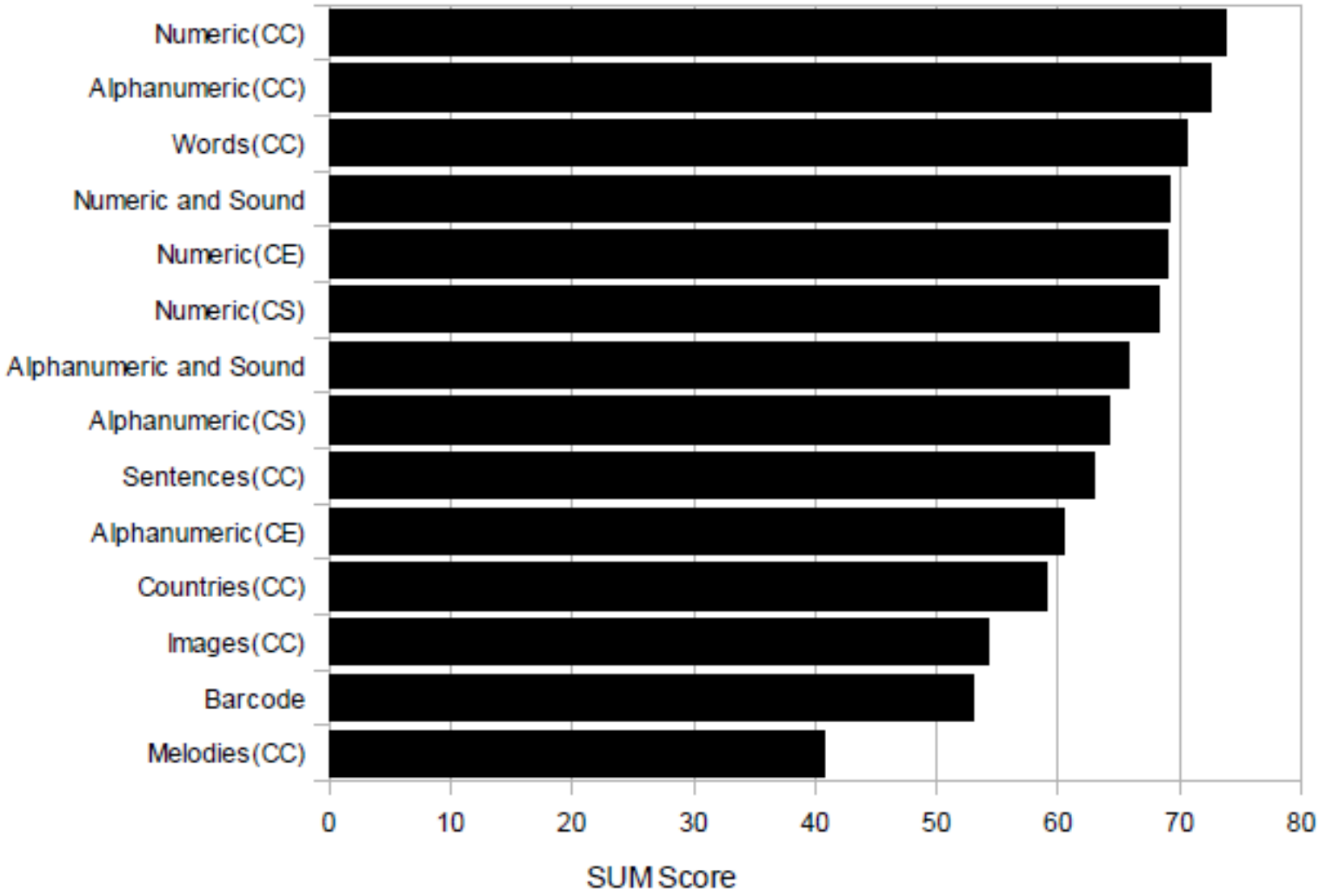

(a) Difficult




(b) Easy

# Outline

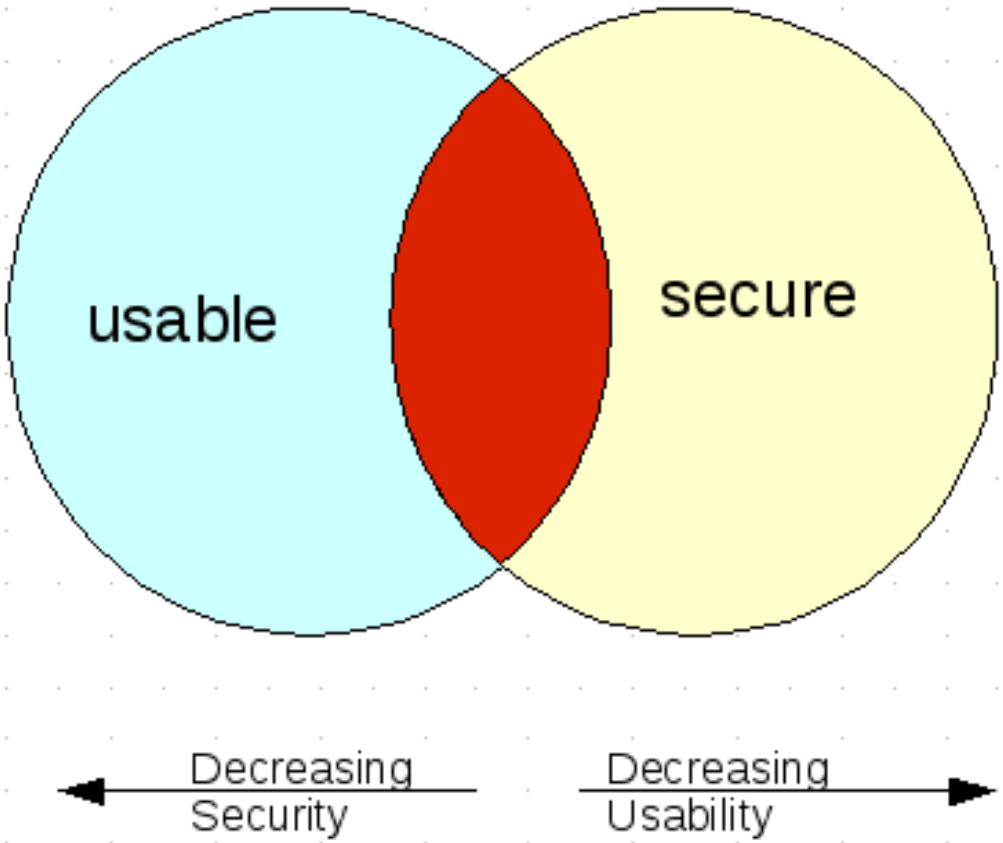
# Analysis and Discussion – SUM Score Ranking



# Analysis and Discussion – Ranking by Security Failures

| | Subject to SF | SF | SUM Score |
|---|---|---|---|
| Numeric(CE) | No | 0 | 69 |
| Alphanumeric(CE) | No | 0 | 60.4 |
| Barcode | No | 0 | 53 |
| Numeric(CC) | Yes | 0 | 73.7 |
| Sentences(CC) | Yes | 0 | 62.9 |
| Countries(CC) | Yes | 0 | 59.1 |
| Images(CC) | Yes | 0 | 54.3 |
| Words(CC) | Yes | 3.3 | 70.6 |
| Numeric & sound | Yes | 3.3 | 69.2 |
| Alphanumeric & sound | Yes | 3.3 | 65.8 |
| Melodies(CC) | Yes | 6.7 | 40.7 |
| Numeric(CS) | Yes | 10 | 68.3 |
| Alphanumeric(CC) | Yes | 13.3 | 72.5 |
| Alphanumeric(CS) | Yes | 20 | 64.2 |

# Discussion and Discussion – Security Vs Usability trade-off



# Discussion – Security Vs Usability Considerations

- User conditioning
- User motivation
- Security failures
- Attentiveness

# Outline

# Conclusion

- Traditional methods are favoured by users
- Currently proposed methods need rethinking about their security/usability
- Security failures are not acceptable
- To achieve human compliance, enforcement is required
- Copy & enter is the best compromise

# THANK YOU

# Conclusion

# Conclusion