# Secure and Usable Out-Of-Band Channels for *Ad hoc* Mobile Device Interactions

Ronald Kainda, Ivan Flechais, A.W. Roscoe

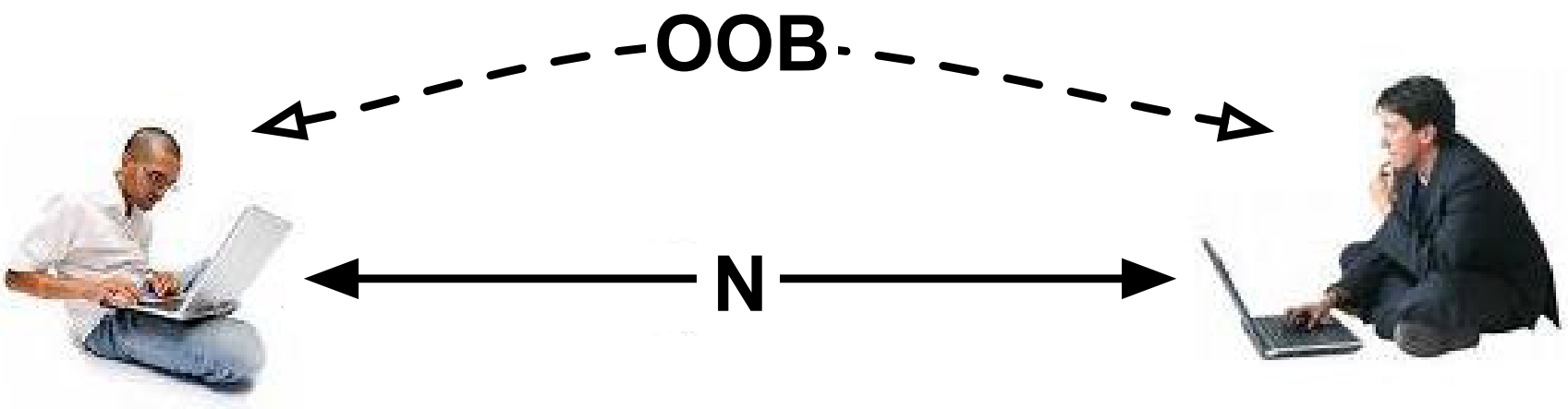
Workshop in Information Security Theory and Practices (WISTP)
University of Passau, Germany

14 April, 2010

# Outline

# *Ad hoc* mobile device interactions

# Human-Interactive Security Protocols (HISP)



# Human-Interactive Security Protocols (HISP)

1. $\forall A \longrightarrow_N \forall A' : A, INFO_A, longhash(A, k_A)$
2. $\forall A \longrightarrow_N \forall A' : k_A$
3. $\forall A \longrightarrow_{OOB} \forall A'$ :users compare *Digest(k*,INFOs)* where k* is the XOR of all the $k'_A s$ for A $\in$ G[1]

- Security is $2^b$
- Increasing $b$ cost usability

[1] *Roscoe et al. 2007*

# Existing OOB methods

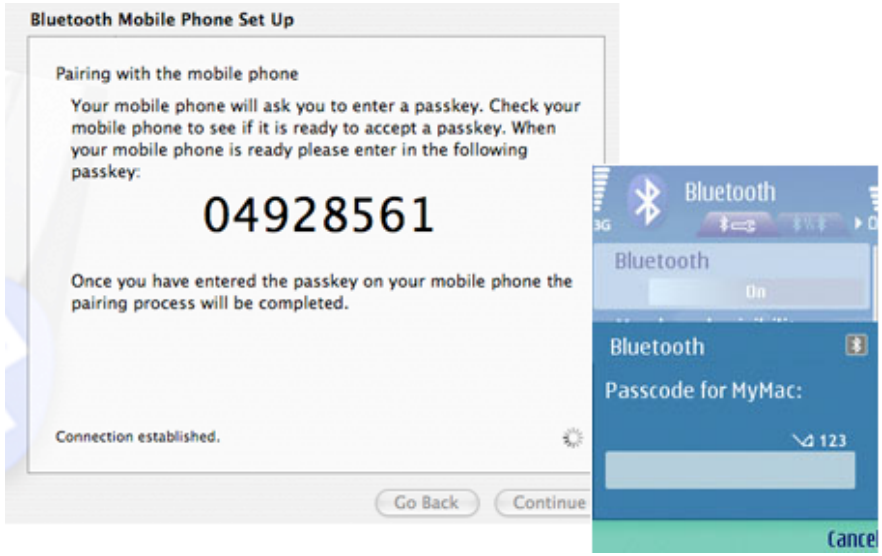
## Manual comparison

- 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
- Security failures

# Existing 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
- Scalability, usability



# Existing OOB methods

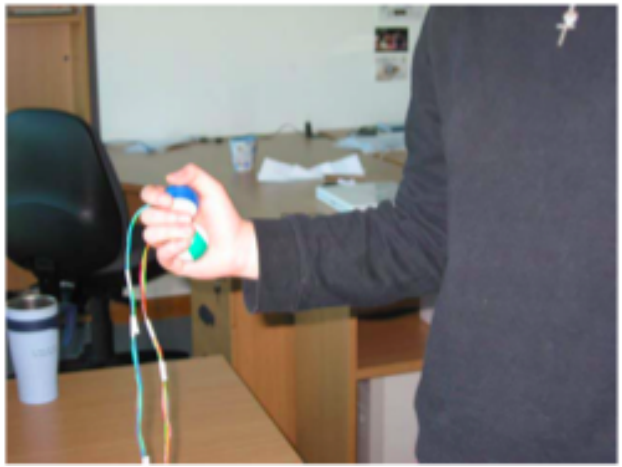
## Auxiliary devices

- 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
- Uniform interfaces, usability

# Existing OOB Methods

**Timing methods**

- Rely on specialised hardware
- Proposed devices include
  - Shaking devices
  - Pressing buttons
- Scalability, usability



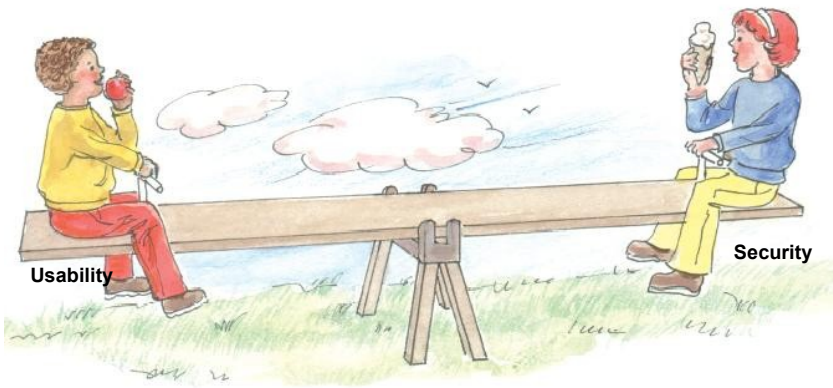
# Existing OOB methods

**Short range directed channels**

- Rely on wireless transmission technologies
- Proposed methods include
  - Infra-red
  - Light
- May require specialised hardware
- Security, scalability

# Problems with current OOB Channels

- Context specific
- Requirement for specialised hardware
- Security and usability
- Scalability



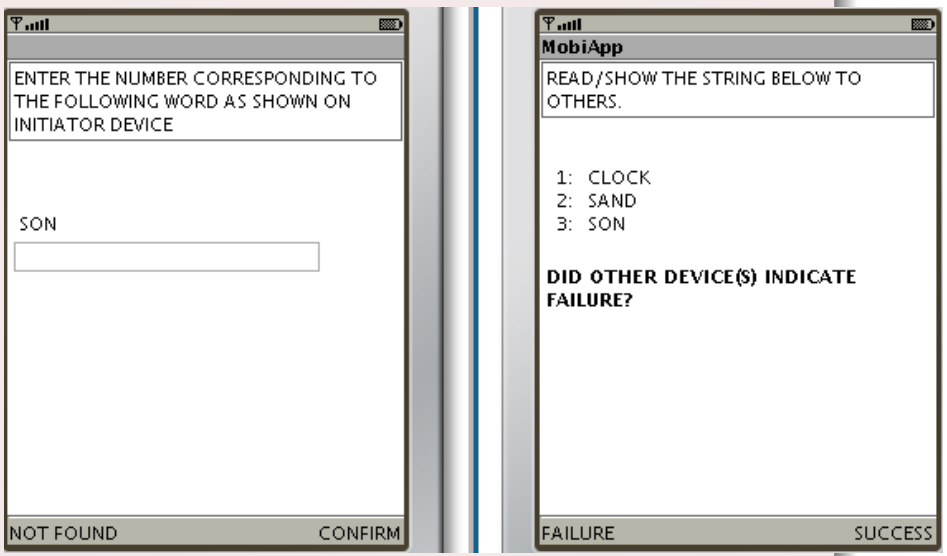
# Proposed OOB —*Word-matching and number-typing*

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

# Proposed OOB —*Word-matching and number-typing*

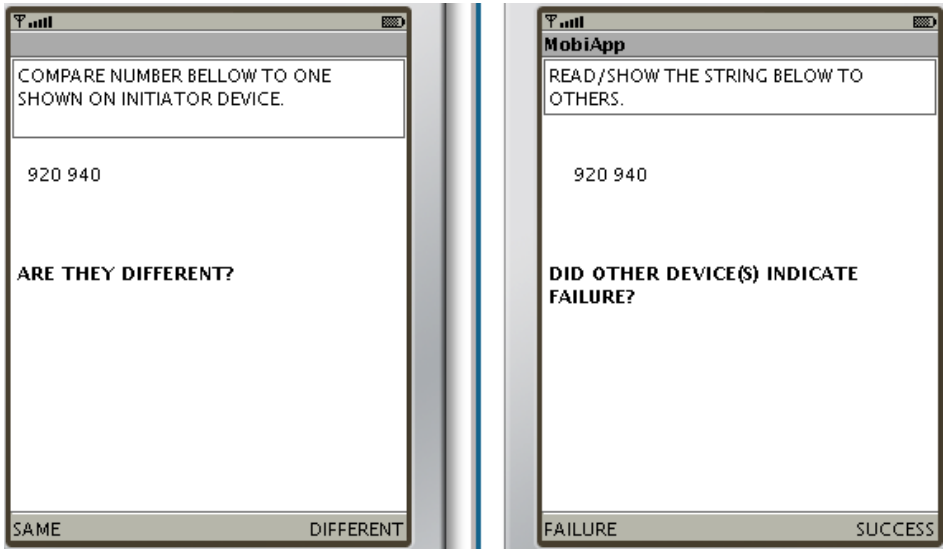
## Potential problems

- Prediction failures
- Word collisions
- Similar sounding words
- Scalable, usable, secure



# Proposed OOB —*Repeated numeric comparison*

- Similar to *manual comparison*
- Not subject to security failures
- Display and button
- Correct response is $2^n$



# Summary of usability study results

- No statistical significance between the two methods in completion times (12.7 and 13.4s mean) ($t(55) = .53$, $p = .598$)
- Ease-of-use: 93% for WMNT, 89% RC
- Preferences: 57% WMNT, 25%RC
- Ratings: no statistical significance ($Z = -0.275$ and $p(2\text{-tailed}) = .78$)
- 13.4s for RC compared to 16.4s reported by Uzun *et al.* for *compare and confirm*
- 12.7s for WMNT compared to 13s reported by Uzun *et al.* for *copy and enter*
- Both methods ranked higher than *compare and confirm* and *copy and enter*

# Applications of proposed methods

- Close/distant devices
- Input/output constrained devices
- Group scenarios
- Larger fingerprints

# Conclusion

- Security and usability should both be embedded in OOB channels
- OOB methods are either secure or usable. Neither are they scalable
- *word-matching and number-typing* and *repeated numeric comparison* achieve all three
- Aplicable to a range of scenarios that other methods may not


THANK YOU