Security Vs Usability: Humans in the loop

Ronald Kainda

St. Cross College Colloquium, University of Oxford

3 November, 2009

Outline

Outline

Definitions

Computer security

deals with the deterrence, avoidance, prevention, detection and reaction to events in and affecting a computer system that are undesirable to the owner of that system (Flechais 2005)

Definitions

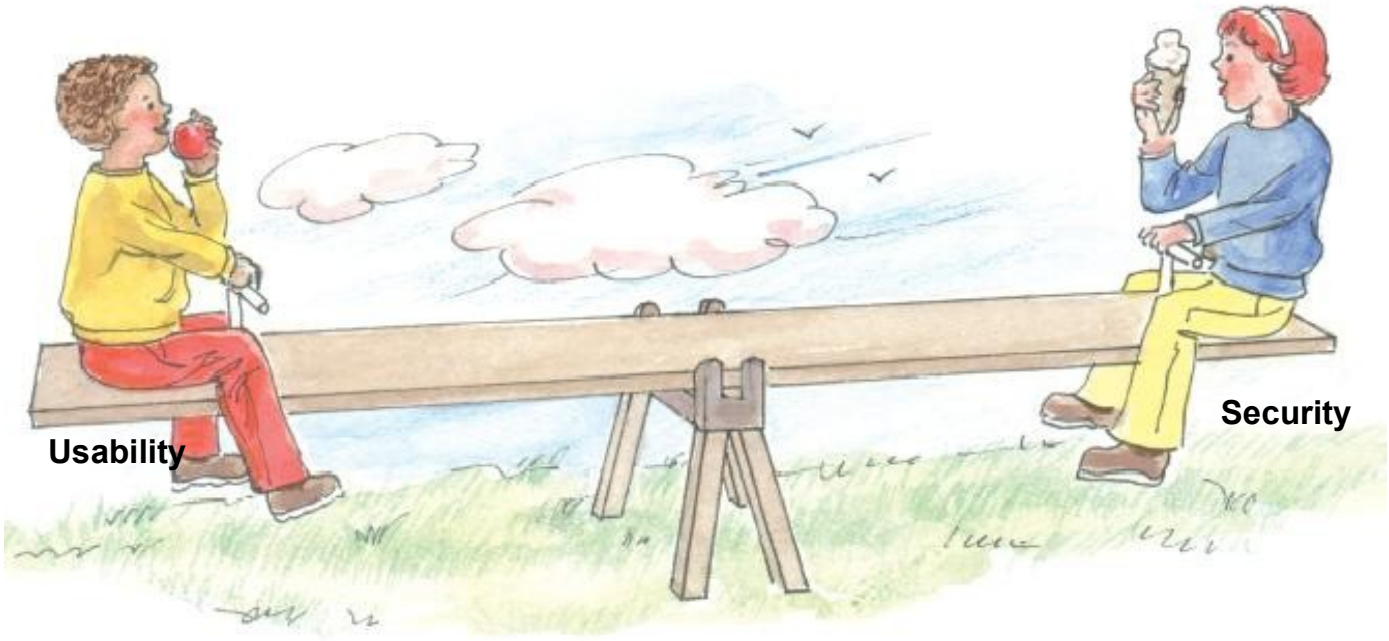
Computer security

deals with the deterrence, avoidance, prevention, detection and reaction to events in and affecting a computer system that are undesirable to the owner of that system (Flechais 2005)

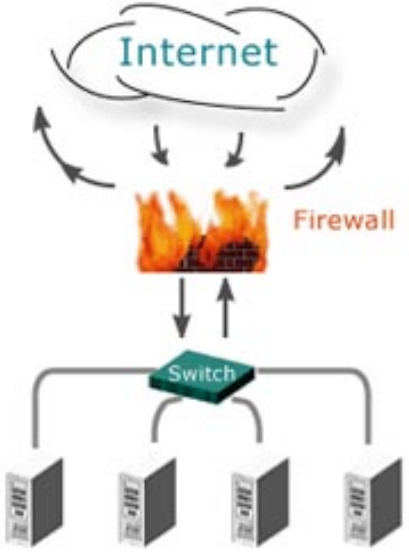
Usability

the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use (ISO 9241-11, 1998)

Security verses Usability?



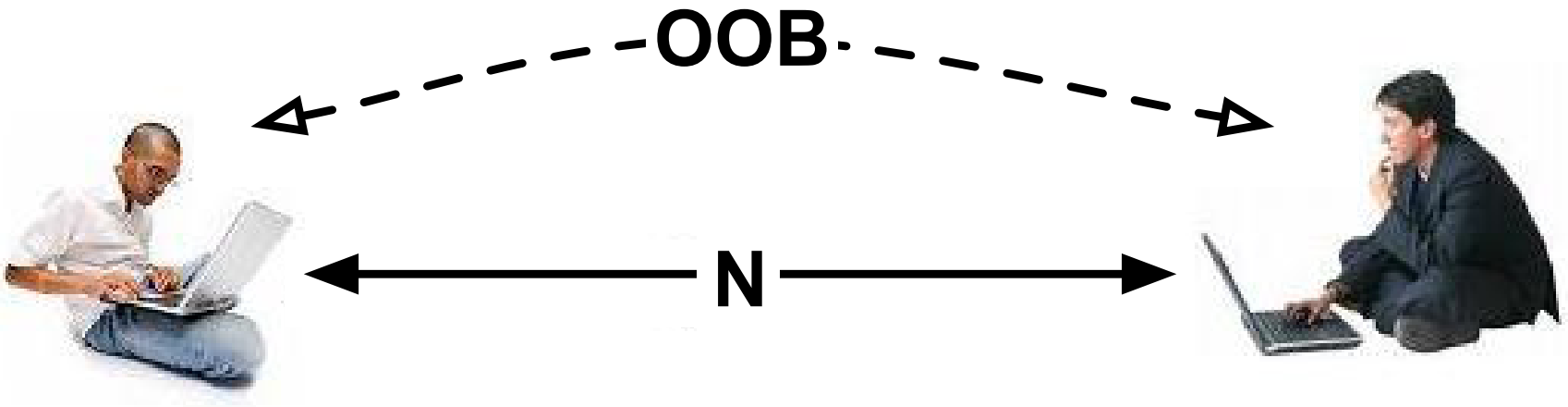
Security - traditional approaches



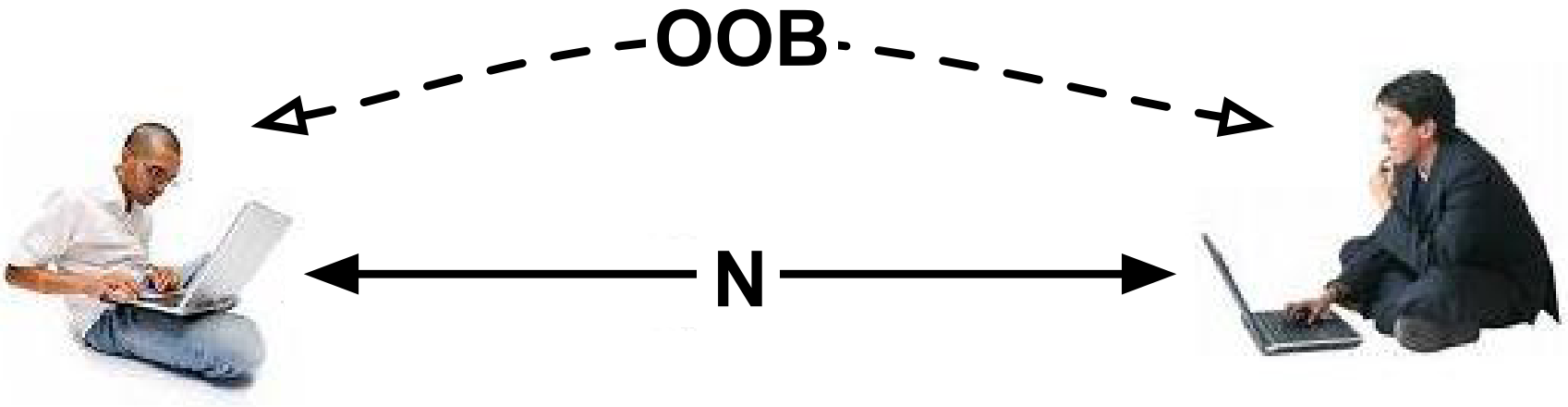
Outline

Mobile device interactions

Security protocols for mobile device interactions



Security protocols for mobile device interactions



... security is only as good as it's weakest link, and people are the weakest link in the chain (Schneier, 2000)

Research Question

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

Proposed OOB Methods

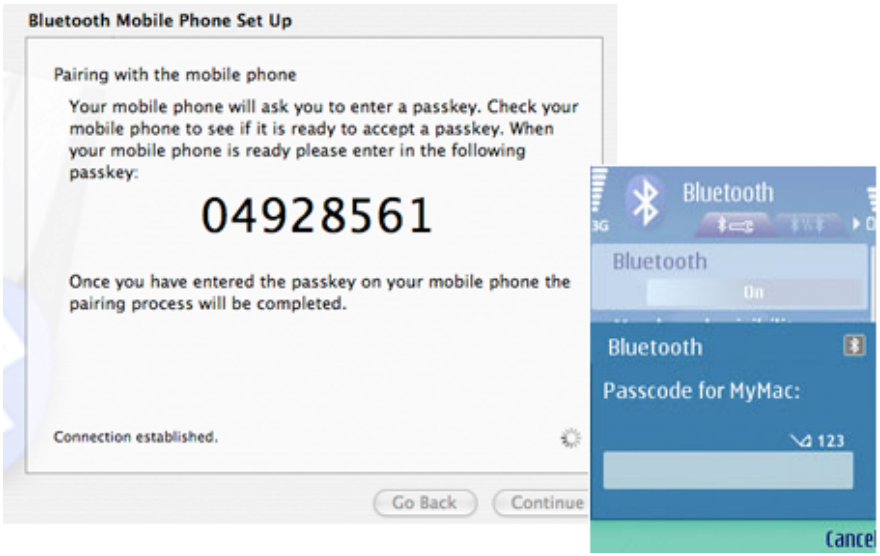
Manual comparison

- 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

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



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

Outline

Tasks

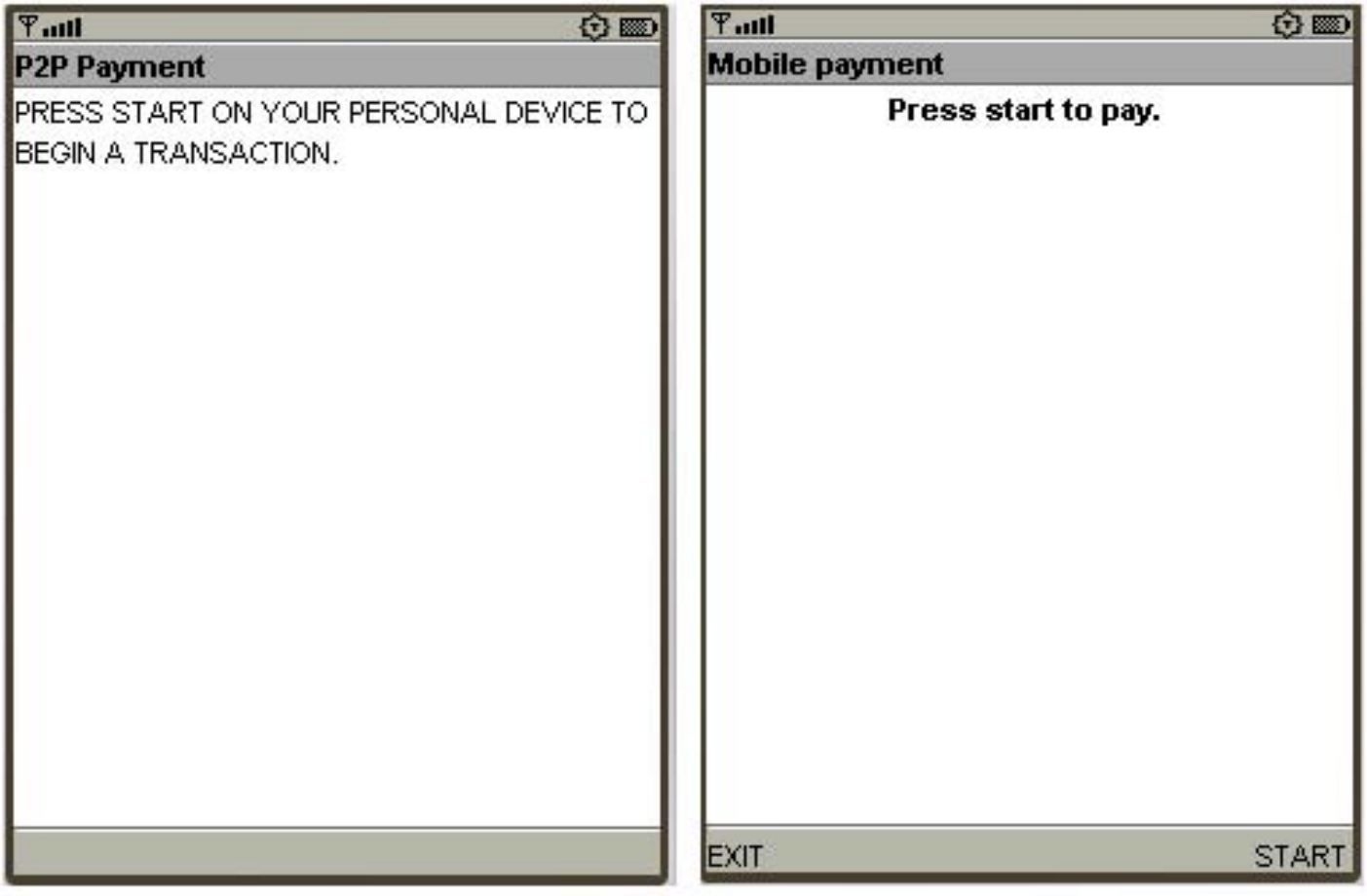


Figure: Step 1

Tasks

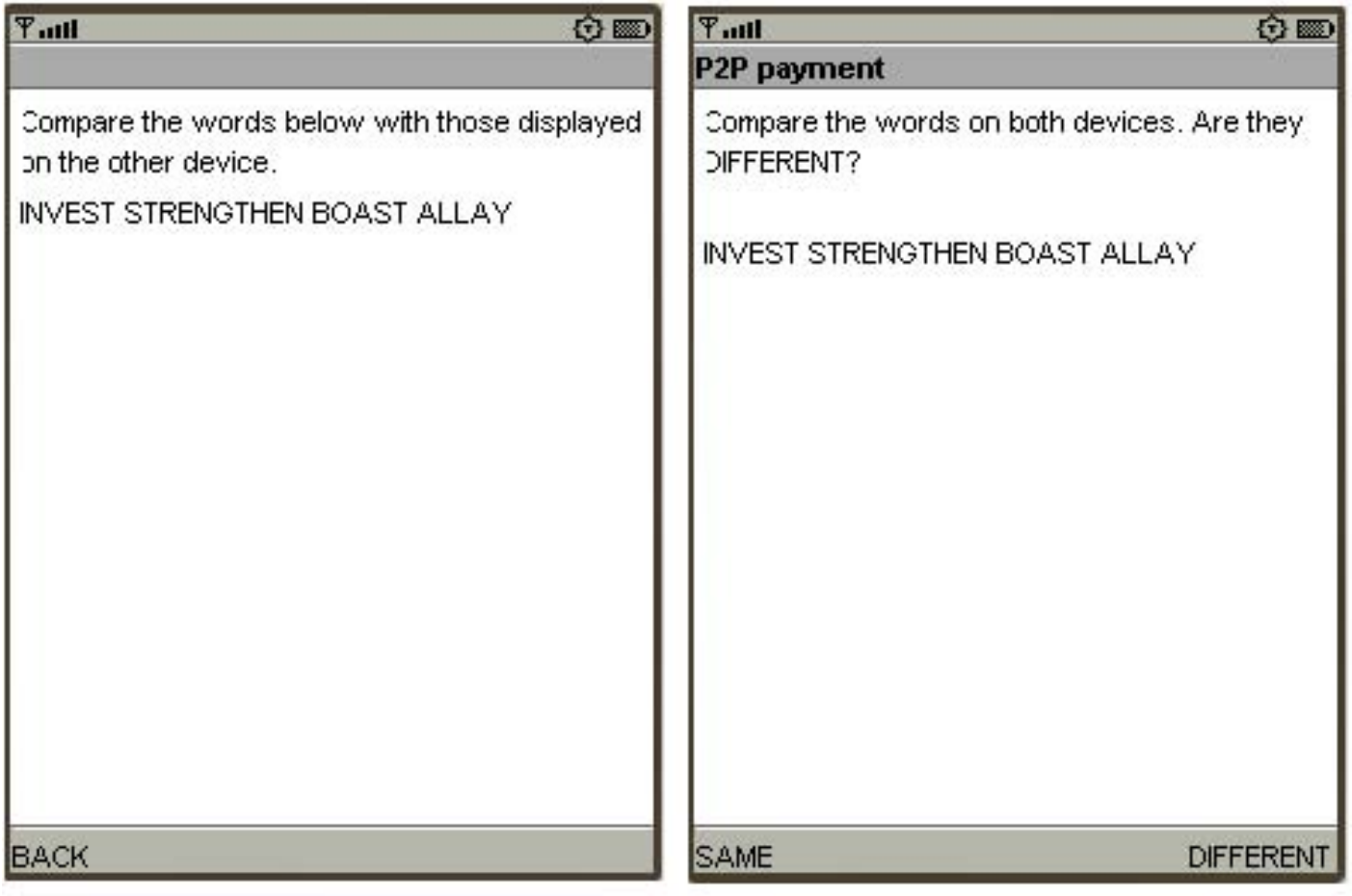
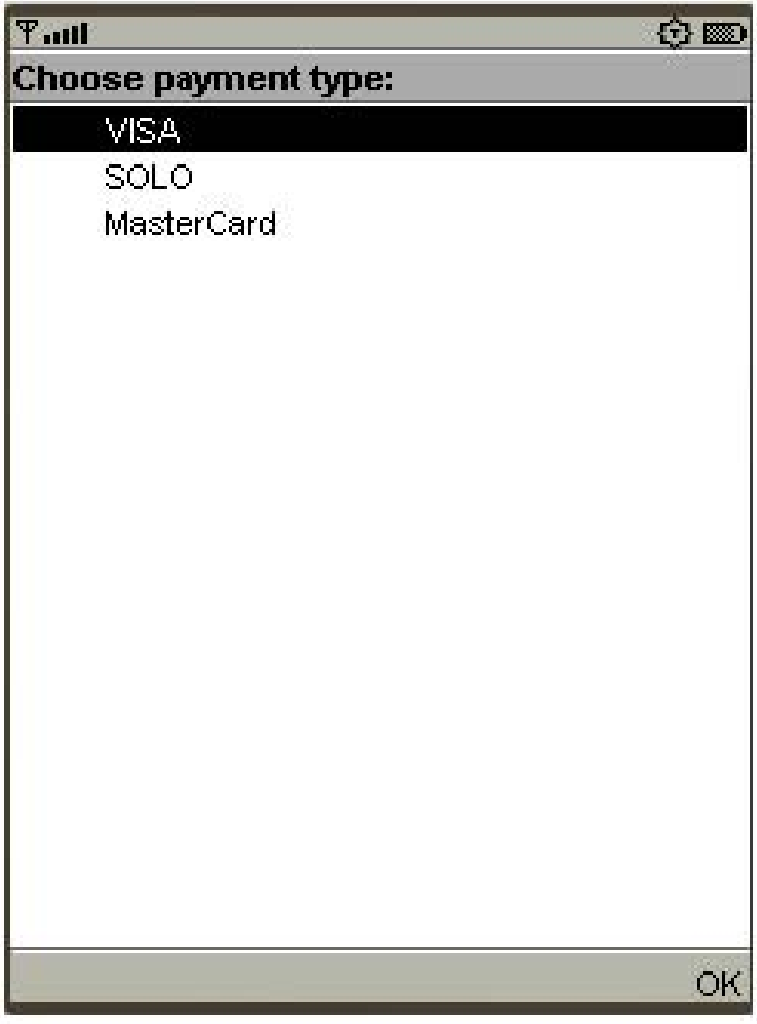


Figure: Step 2

Tasks



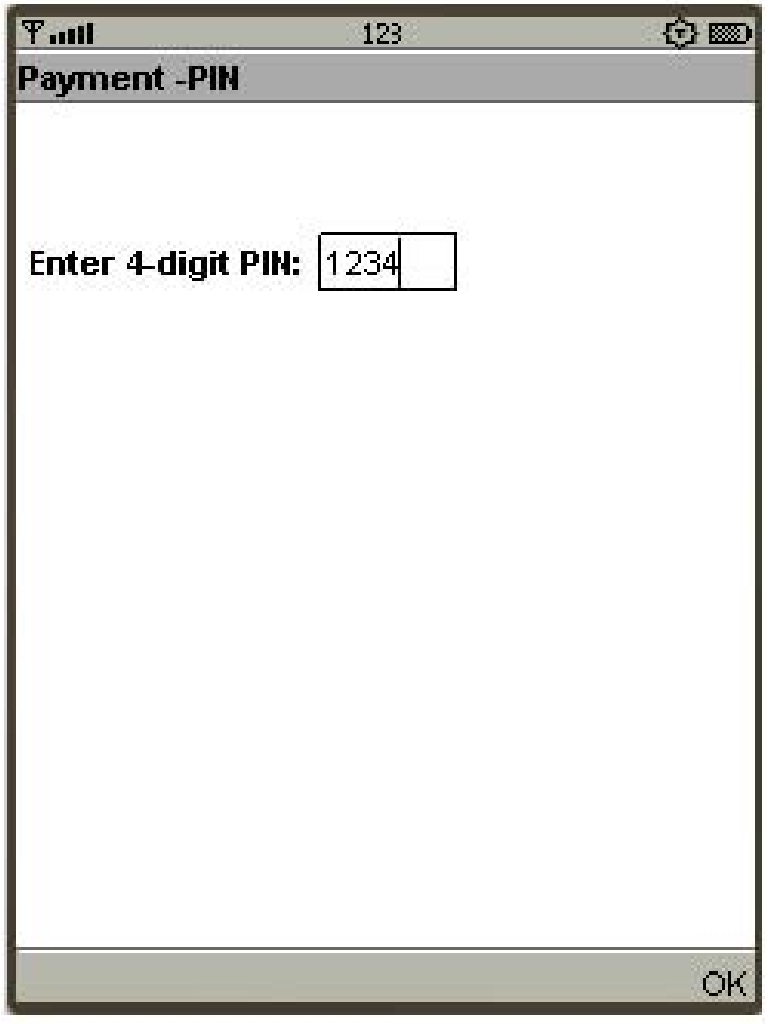


Figure: Step 3 and 4

Procedure: Tasks

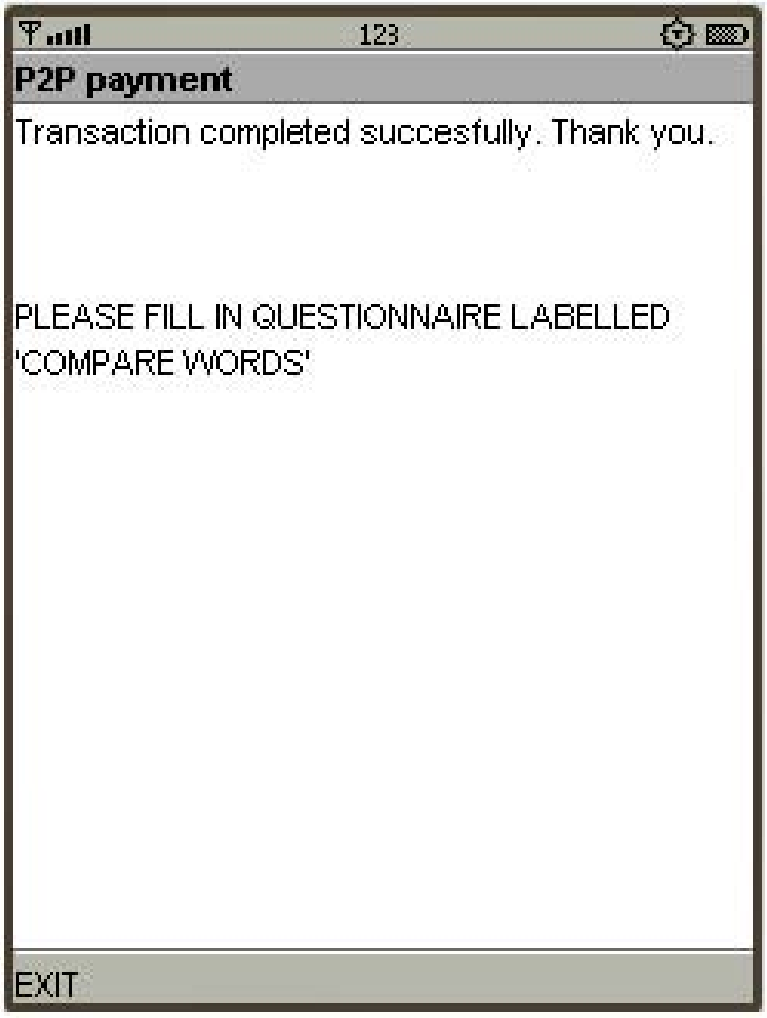
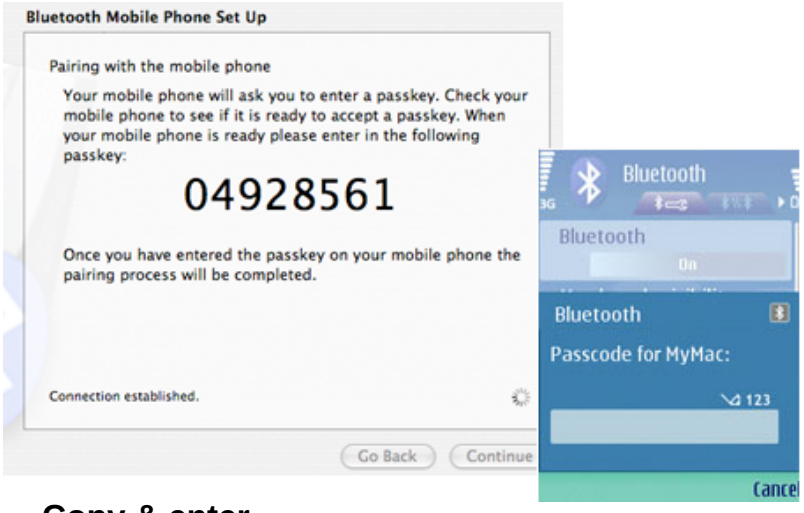


Figure: Step 5 and 6

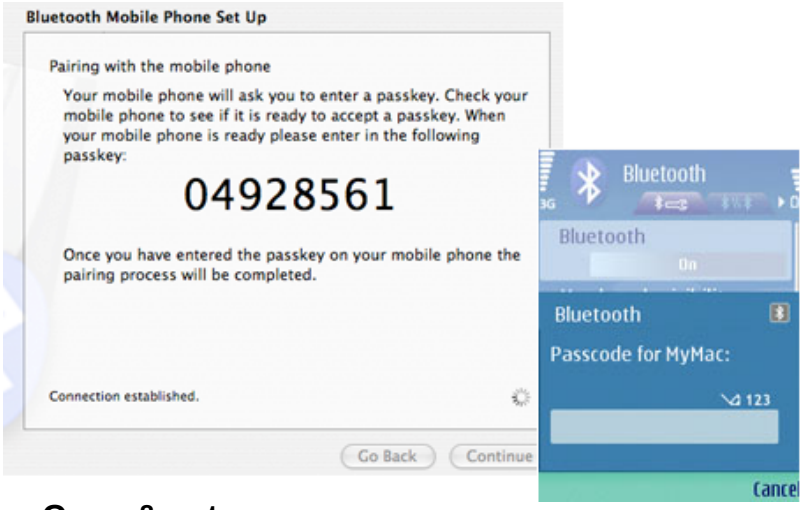
Outline

Results

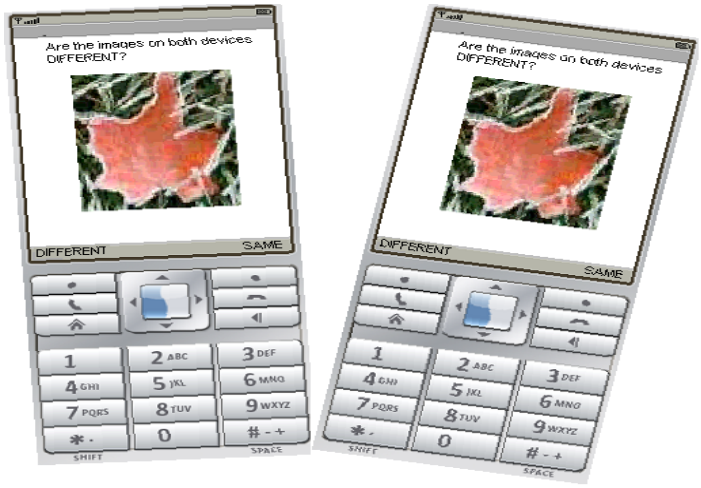


Copy & enter

Results

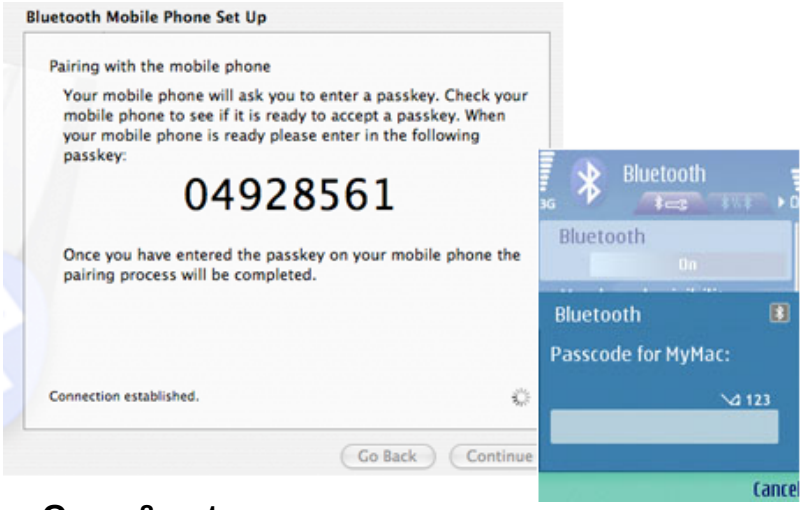


Copy & enter

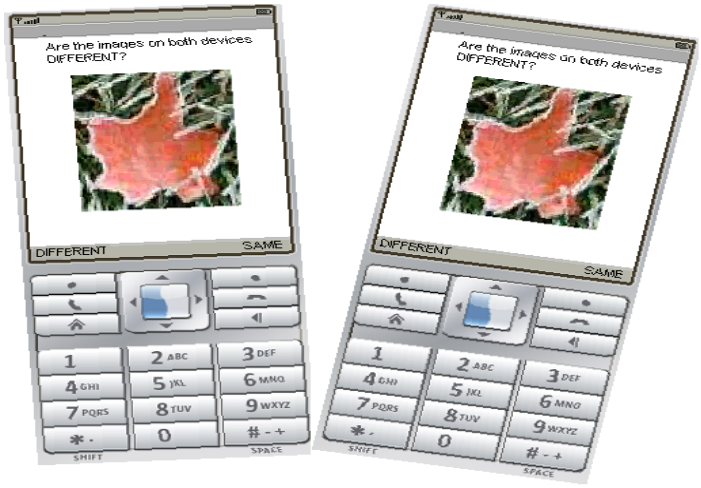


Compare & confirm

Results



Copy & enter

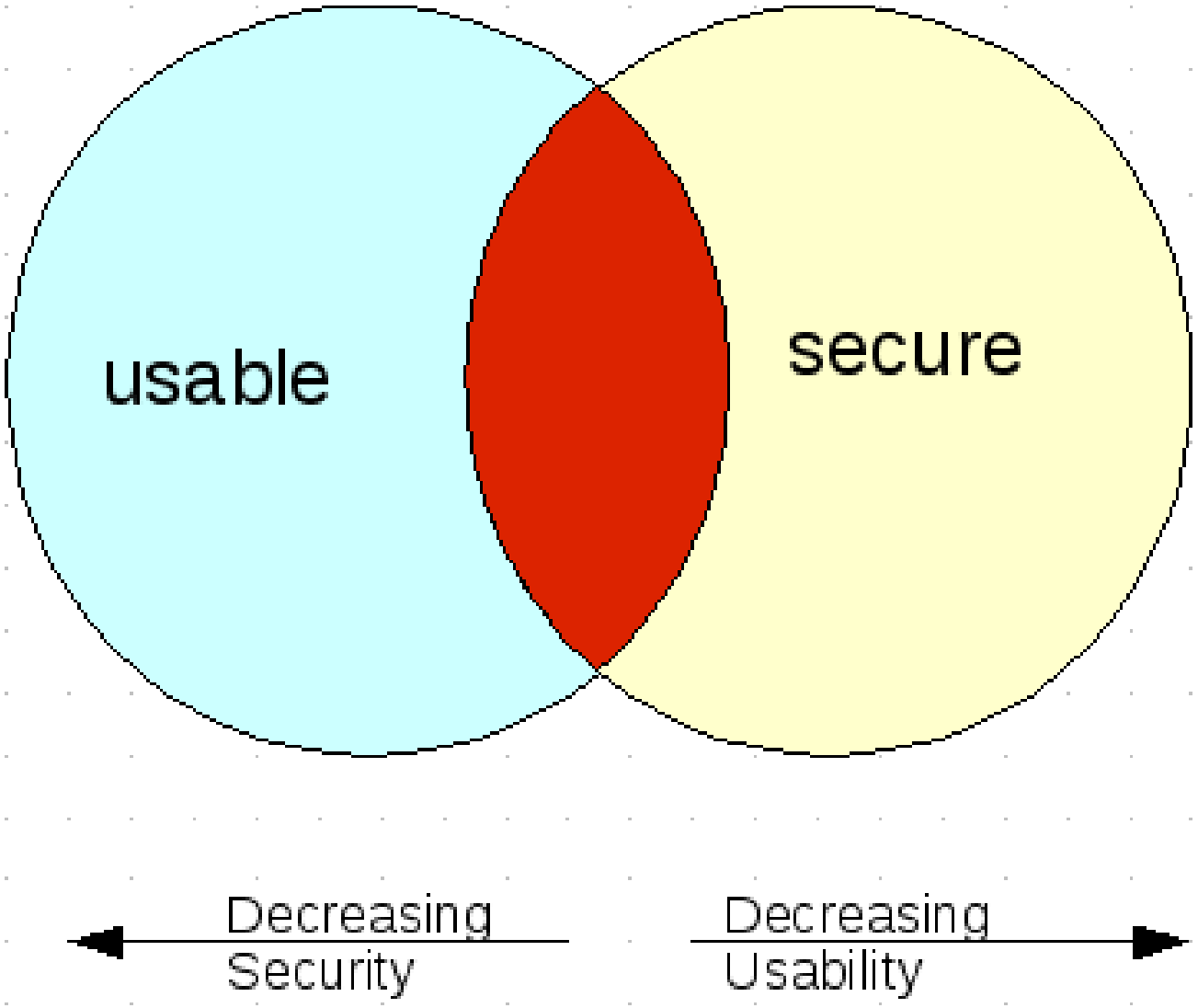


Compare & confirm

Auxiliary method

Outline

Security Vs usability considerations



Outline

Conclusion

- Secure systems are socio-technical (Sasse et al.)
- Security may depend on human effort
- Human mistakes may result in security failures
- Achieving effective security goes beyond formal proofs
- Increasing technical security may reduce effective security

THANK YOU