Secure Mobile *Ad-hoc* Interactions: Reasoning About Out-Of-Band (OOB) Channels

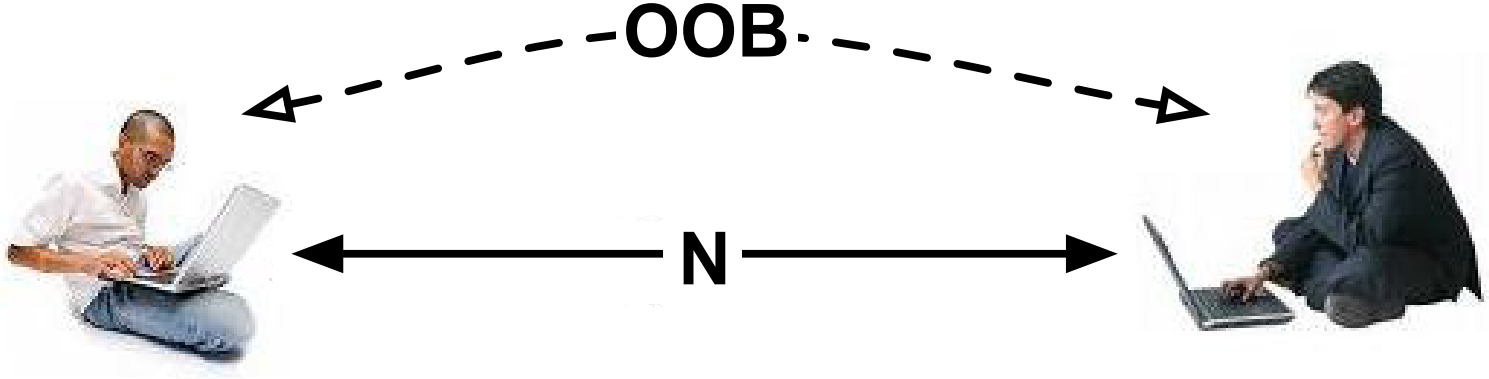
Ronald Kainda, Ivan Flechais, A.W. Roscoe

International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)
University of Helsinki, Finland

17 May, 2010

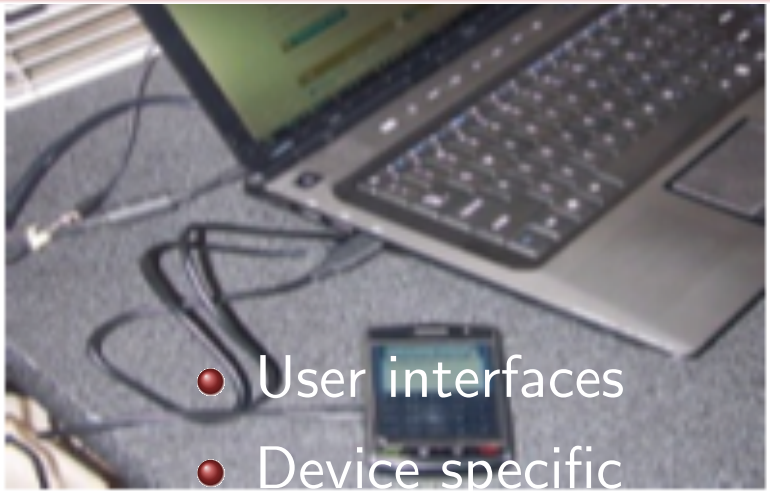
Outline

Human-Interactive Security Protocols



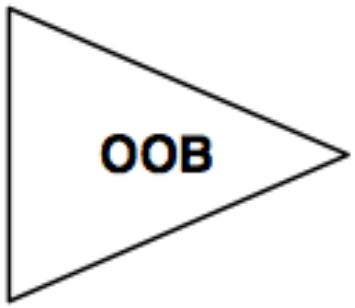
OOB = Out-Of-Band Channel, N = Normal Channel

Limitations of existing OOB channels

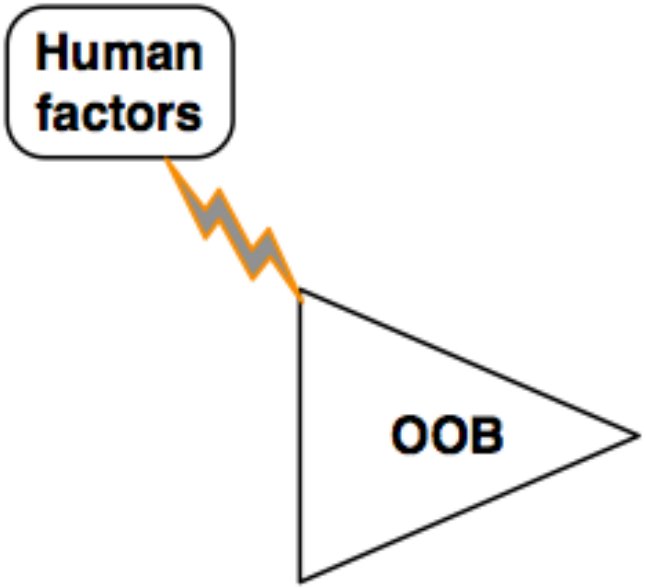


- User interfaces
- Device specific
- Similar devices
- Universal solution
- Scenario specific

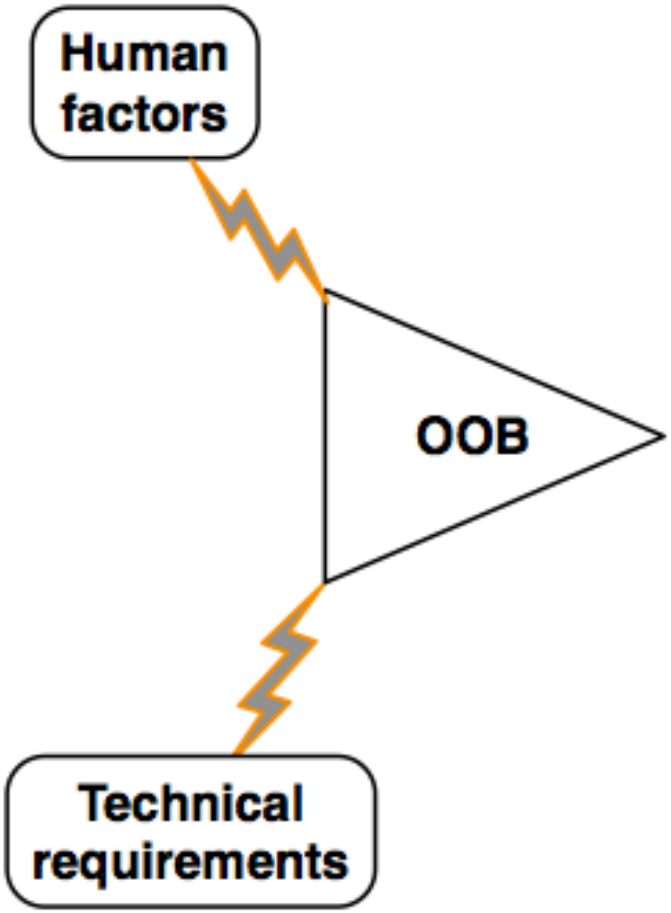
OOB channels - factors to consider



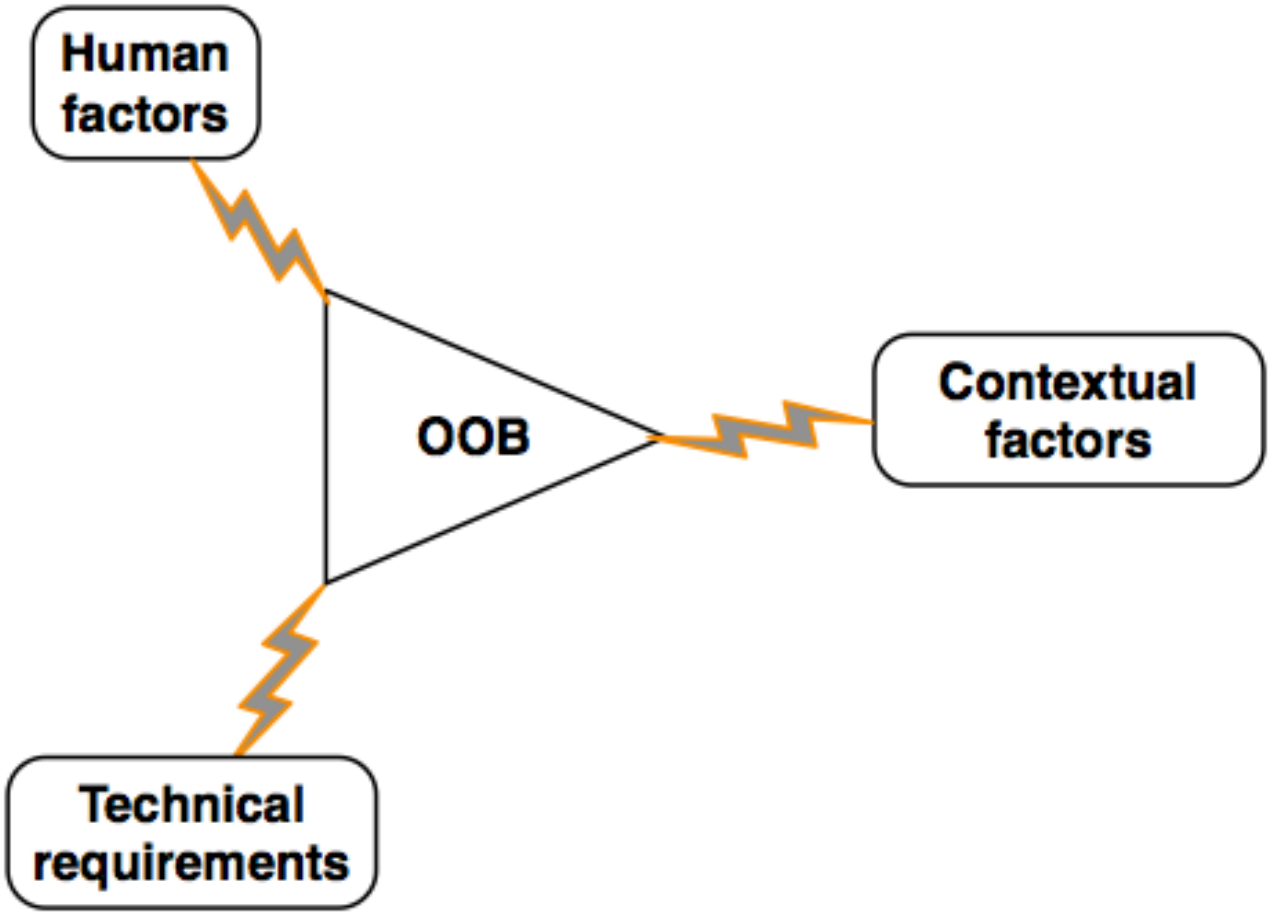
OOB channels - factors to consider



OOB channels - factors to consider



OOB channels - factors to consider



Technical and contextual factors

Contextual

- Social, physical, technological *etc.*
- Matching needs to immediate security concerns
- Changing context is a challenge

Technical and contextual factors

Contextual

- Social, physical, technological *etc.*
- Matching needs to immediate security concerns
- Changing context is a challenge

Technical

- Vulnerable to non-malicious users
- Complexity is bad for security
- Require technical expertise
- Security = technical solution + correct application within context

Human factors

Personal variables

- Aware of security needs, unmotivated
- Users misconceive risk
- Social countermeasure
- Are vulnerable to lapses (human error?)

Human factors

Personal variables

- Aware of security needs, unmotivated
- Users misconceive risk
- Social countermeasure
- Are vulnerable to lapses (human error?)

Intentions

- Willingness to carry out a particular behaviour
- Attitude (beliefs) and motivation
- Security must be aligned with user goals

Human factors

Personal variables

- Aware of security needs, unmotivated
- Users misconceive risk
- Social countermeasure
- Are vulnerable to lapses (human error?)

Intentions

- Willingness to carry out a particular behaviour
- Attitude (beliefs) and motivation
- Security must be aligned with user goals

Capability

- Perception
- Physical, mental, technological

OOB channels

Target goals

- Secure
- Scalable
- Adaptation
- Fit for purpose

Application of framework

Application

- Fits in User-Centred Design (UCD) process
  - Analysis, design, evaluate
- Evaluation may be against theoretical specifications or empirical
- Outcome of evaluation used as feedback

Summary and conclusion

Summary

- Proposed methods limited in application
- OOB channels must be evaluated against technical security requirements, human factors, and context
- Proposed framework identifies main elements
- Framework fits into UCD process
- Possibility of extending to other secure systems


THANK YOU