

Security & Trust in Mobile Interactions

A study of Users' Perceptions & Reasoning

Tim Kindberg, Abigail Sellen & Erik Geelhoed
HP Labs, Bristol

Spontaneous Interaction

- Luigi's restaurant
 - Unfamiliar: first visit
 - Semi-public space
- Pay for meal electronically, with "e-wallet"
- Pay when ready

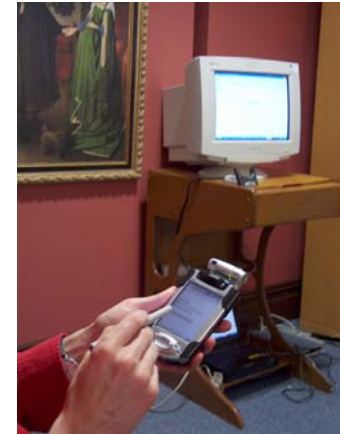


Questions of Trust

- Perceived vulnerability to incorrect system behaviour (malicious or otherwise)
- Affect desirability/usability?
- Most salient points of vulnerability?
 - Reasoning?
- Are responses a function of target (device) or connection method?

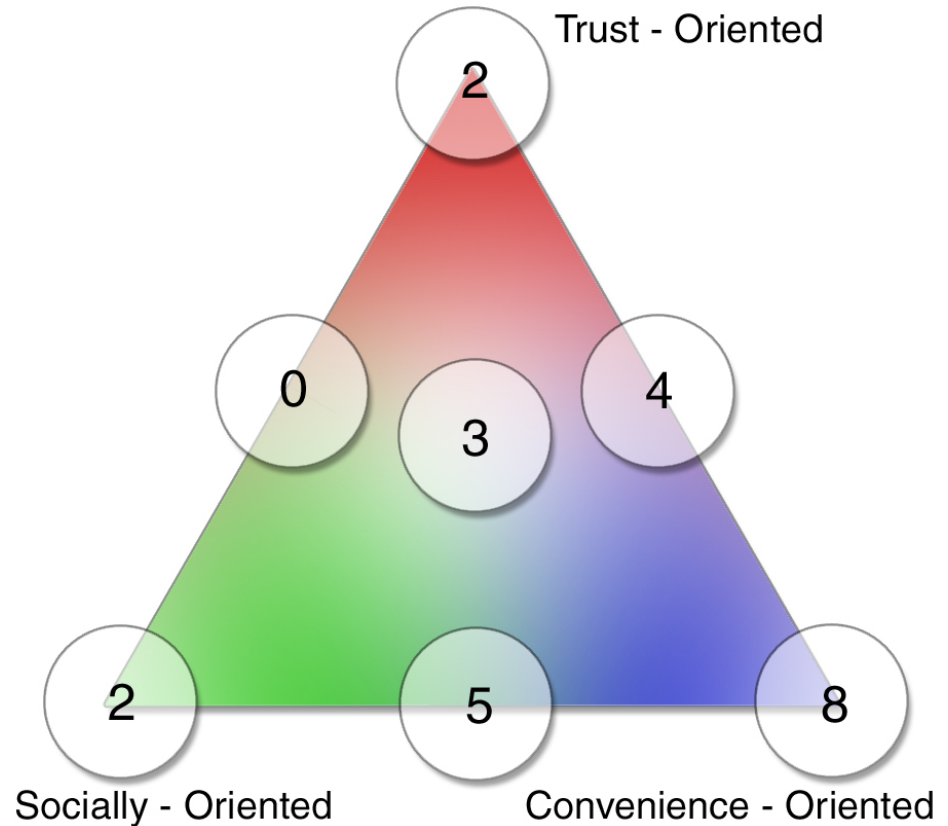
Configurations

- Kiosk/docked
- Kiosk/wireless
- Waiter/docked
- Waiter/wireless
- Barcode



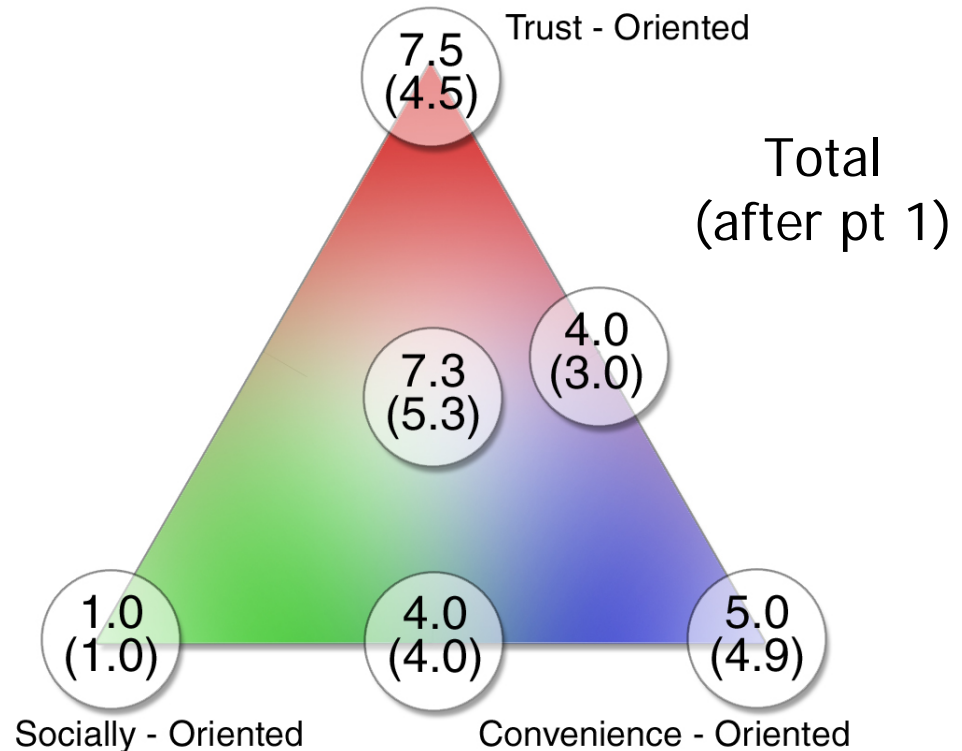
Clusters of Subjects by Rationale

- Coded and counted statements during ranking exercise



Awareness and Trust

- Awareness = count of points of vulnerability
- Trust-oriented raise new points given opportunity
- **Convenience-oriented are quite trust-aware**
- Little re-ranking at end (7 overall, 4 for trust reasons)



Points of vulnerability

1. E-wallet
2. Human agent
3. Communications link
4. Spoofed receiving device
5. Attack on receiving device
6. Doubt about payment
7. Context
8. Other

(Ranked by number of mentions)

Wireless vs docked connections

- Which is more trustworthy?
 - 8 dock, 3 wireless, 13 no opinion stated
- **Wireless ratings significantly > docked for 7 of 12 concern probes**

“It would be easier to take information off it if it was physically connected to another device.”

“Unless you physically walk up to the station and dock and have a look I wouldn’t know where it’s gone – it [the information] just disappears into oblivion.”

Kiosk vs handheld

- Which is more trustworthy?
 - 7 kiosk, 1 handheld, 16 no opinion stated or indeterminate
- Negligible significant diffs in concern ratings

“It’s a psychological thing. It’s the fact that somebody’s there so **you’re paying this person as opposed to something you don’t know.**”

“There isn’t a person there, there’s a machine. When you go to a hole in the wall, you think: **a machine isn’t going to do anything untoward to you.** Machines are not programmed to do that, machines are just programmed to do a certain thing.”

Barcode vs rest

- Which is more trustworthy?
 - 3 barcode, 2 others, 19 no opinion stated or indeterminate
- **Barcode concern ratings for eavesdropping mid-way between docked methods (significantly lower than wireless)**

“No-one else is there and it’s all done in front of you.”

“Someone could put a different barcode on the table which could make the payment go somewhere else.”

Summary

- Important to get social & convenience factors right
- Loose relationship between perceptions & actual risks
 - Poor understanding / awareness on average
- Significant differences between configurations
 - Trust what is visible, tangible & apparently human-free

Research implications

- Study with more realistic threats & costs
- “Tangible and visible” – but socially acceptable – protocols for device association
 - (See talk tomorrow)
- Authenticating physical hyperlinks

Thank you!

tim.kindberg,abigail.sellen,erik.geelhoed@hp.com

tag:timothy@hpl.hp.com,2004:presentations:UK-UbiNet:Luigis

