copenhagen goto; conference

Mobile App Security Techniques and Traps

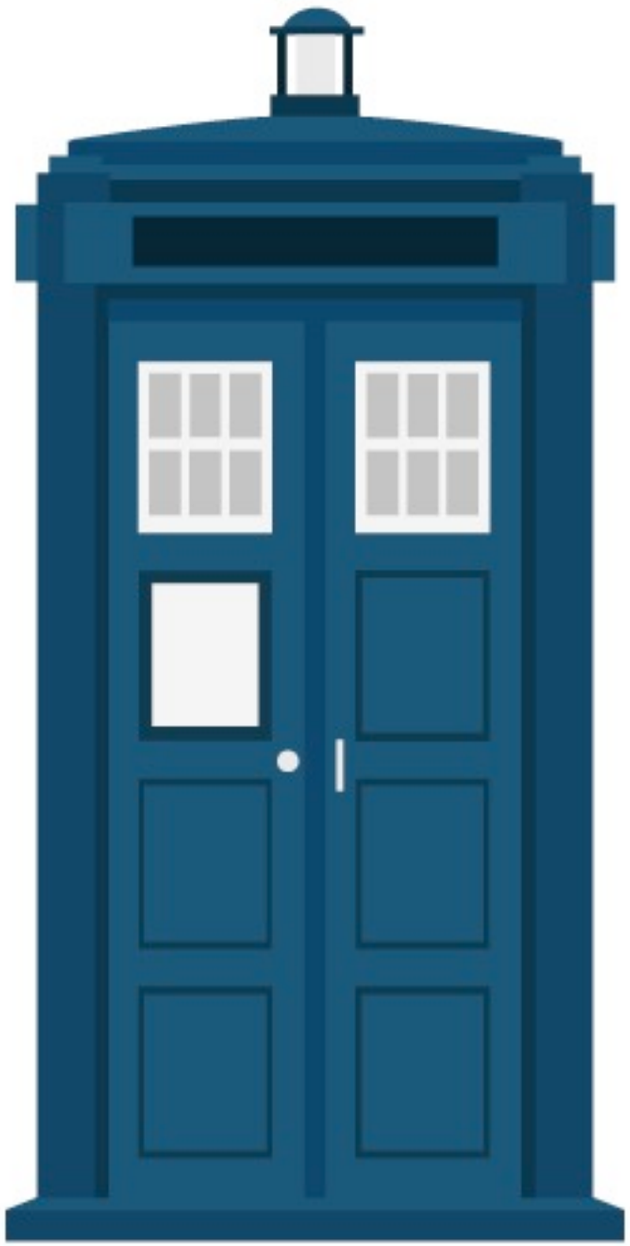
Graham Lee / @secboffin
Smartphone Security Boffin, The Lab @O2

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

gotocon.com

No code

No code



State of the Union

State of the Union

- 1875: UK patent application for telephone

State of the Union

- 1875: UK patent application for telephone
- 2007: Phones got good enough to be useful

State of the Union

- 1875: UK patent application for telephone
- 2007: Phones got good enough to be useful
- 2009ish: Cell networks got good enough to use phones on

State of the Union

- 1875: UK patent application for telephone
- 2007: Phones got good enough to be useful
- 2009ish: Cell networks got good enough to use phones on
- Despite apparent novelty, most security problems already existed:

The problems

The problems

- Who gets to see/change my data?

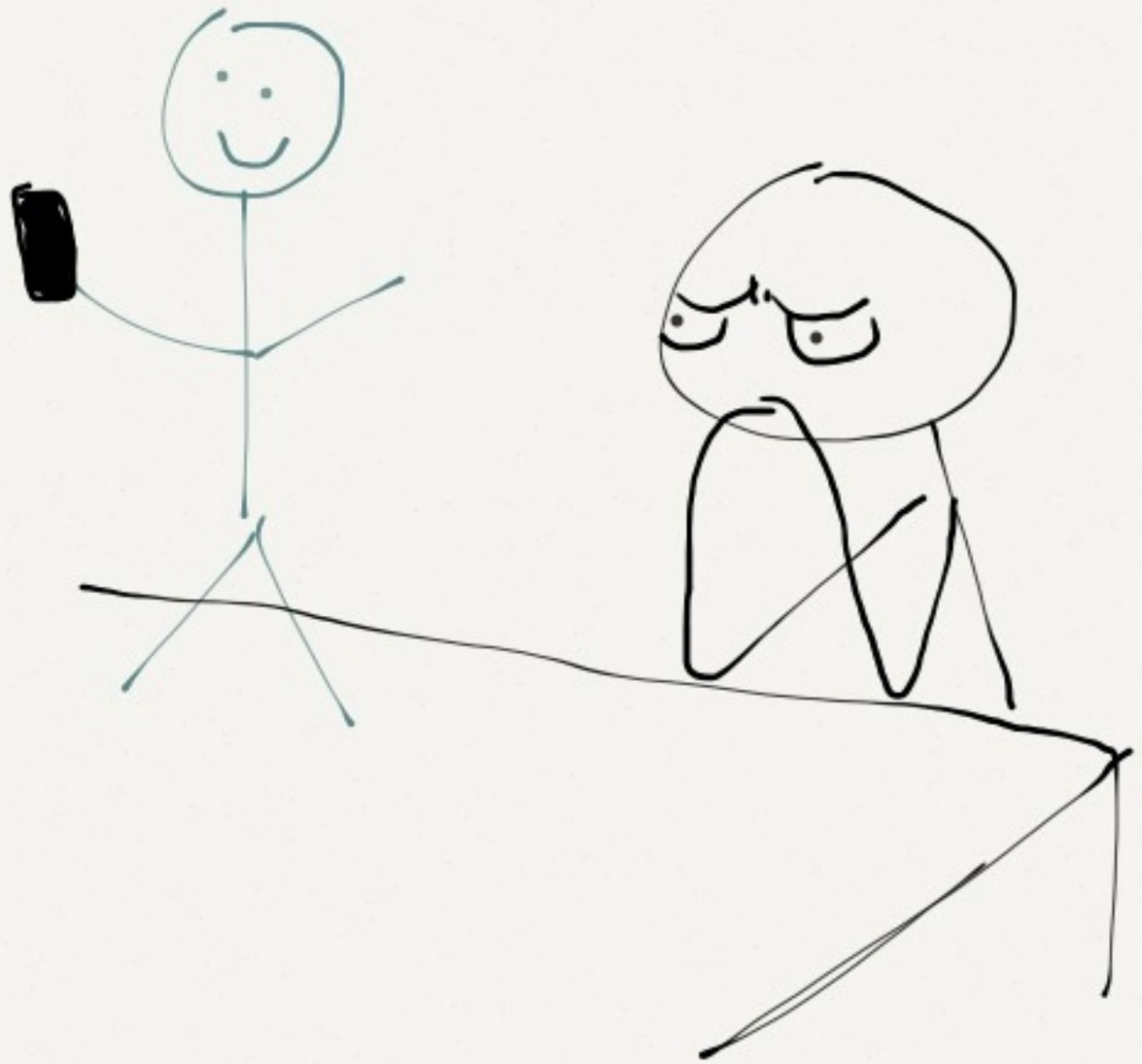
The problems

- Who gets to see/change my data?
- I like sharing things, but only on my terms.

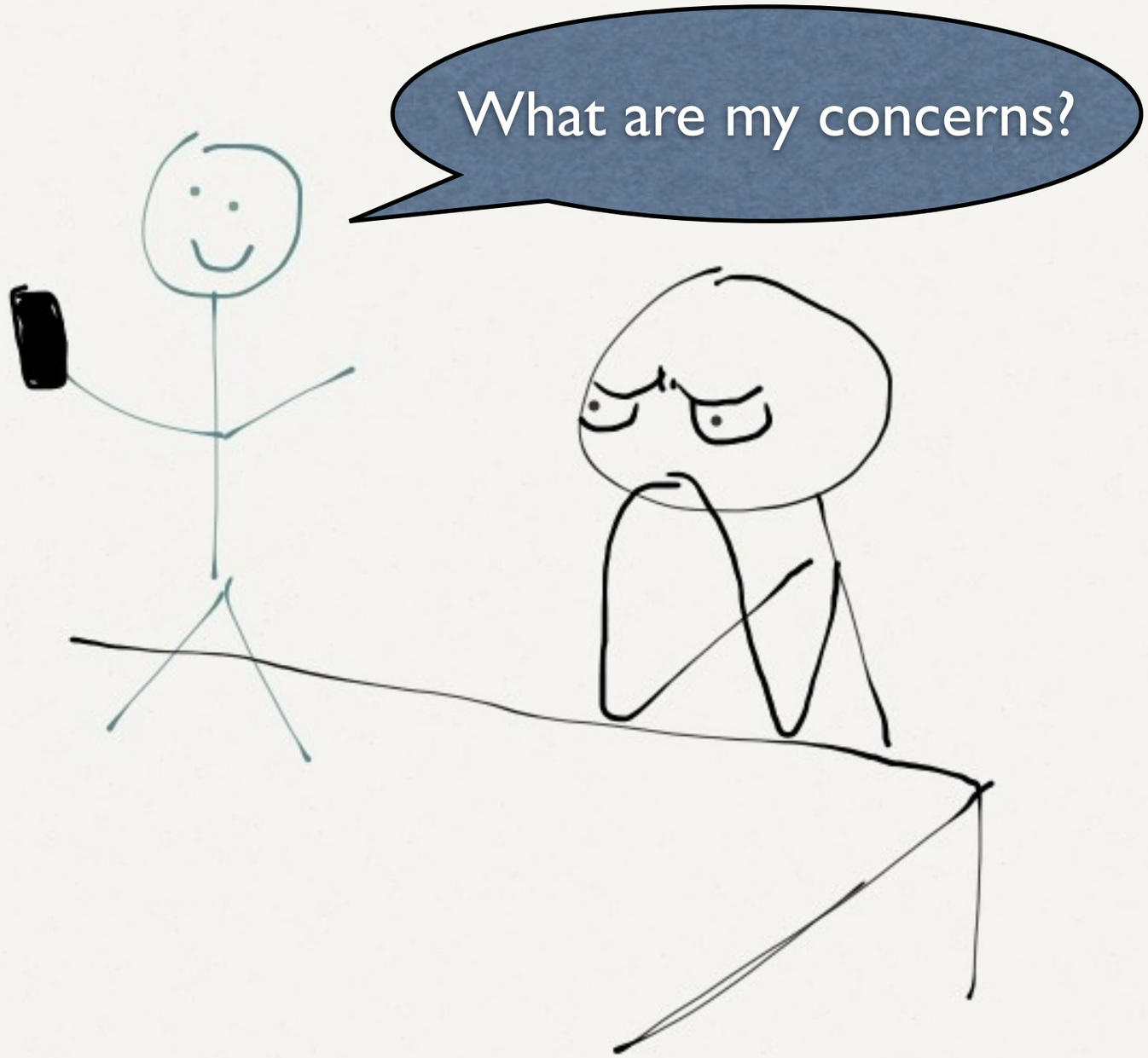
The problems

- Who gets to see/change my data?
- I like sharing things, but only on my terms.
- (these are the same problem stated twice)

Model Your User

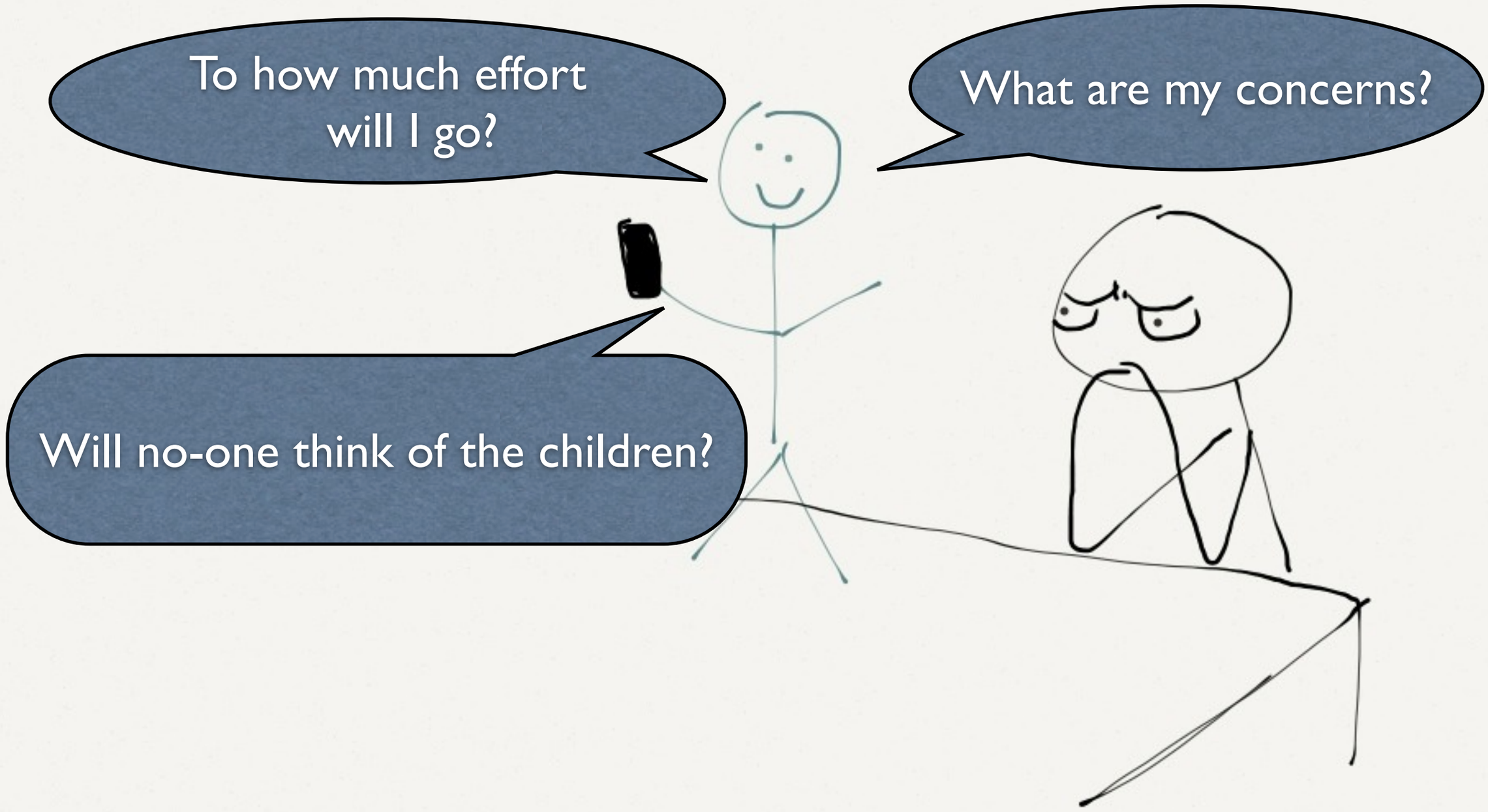


Model Your User



Model Your User

Model Your User

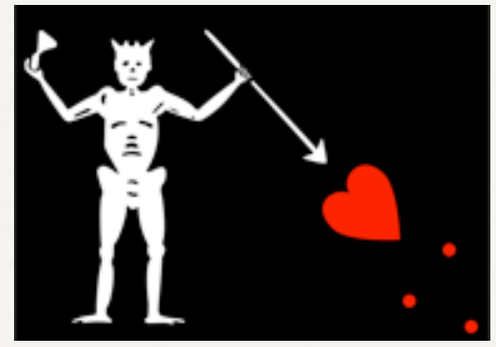


Model Your User

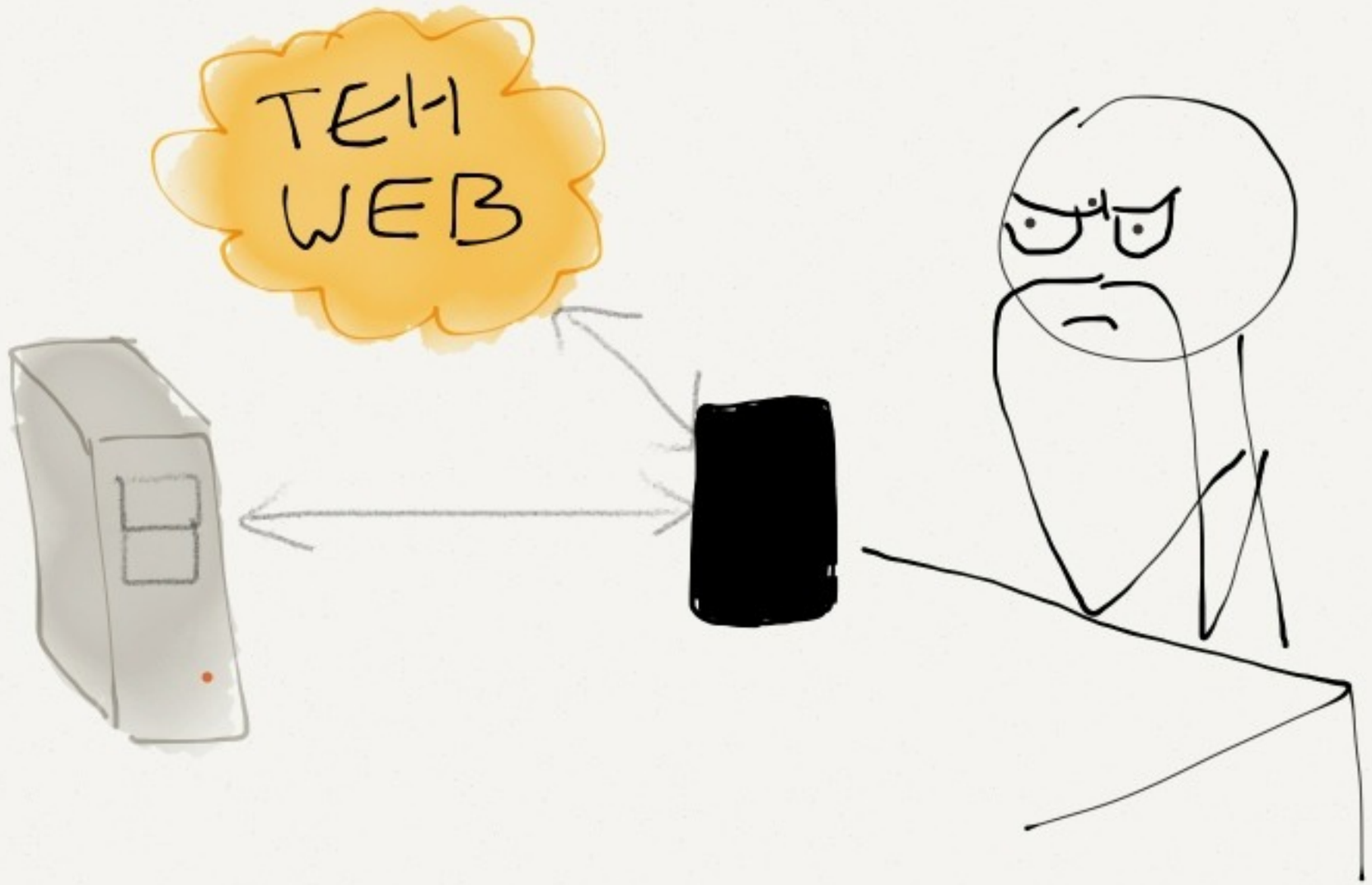
To how much effort will I go?

What are my concerns?

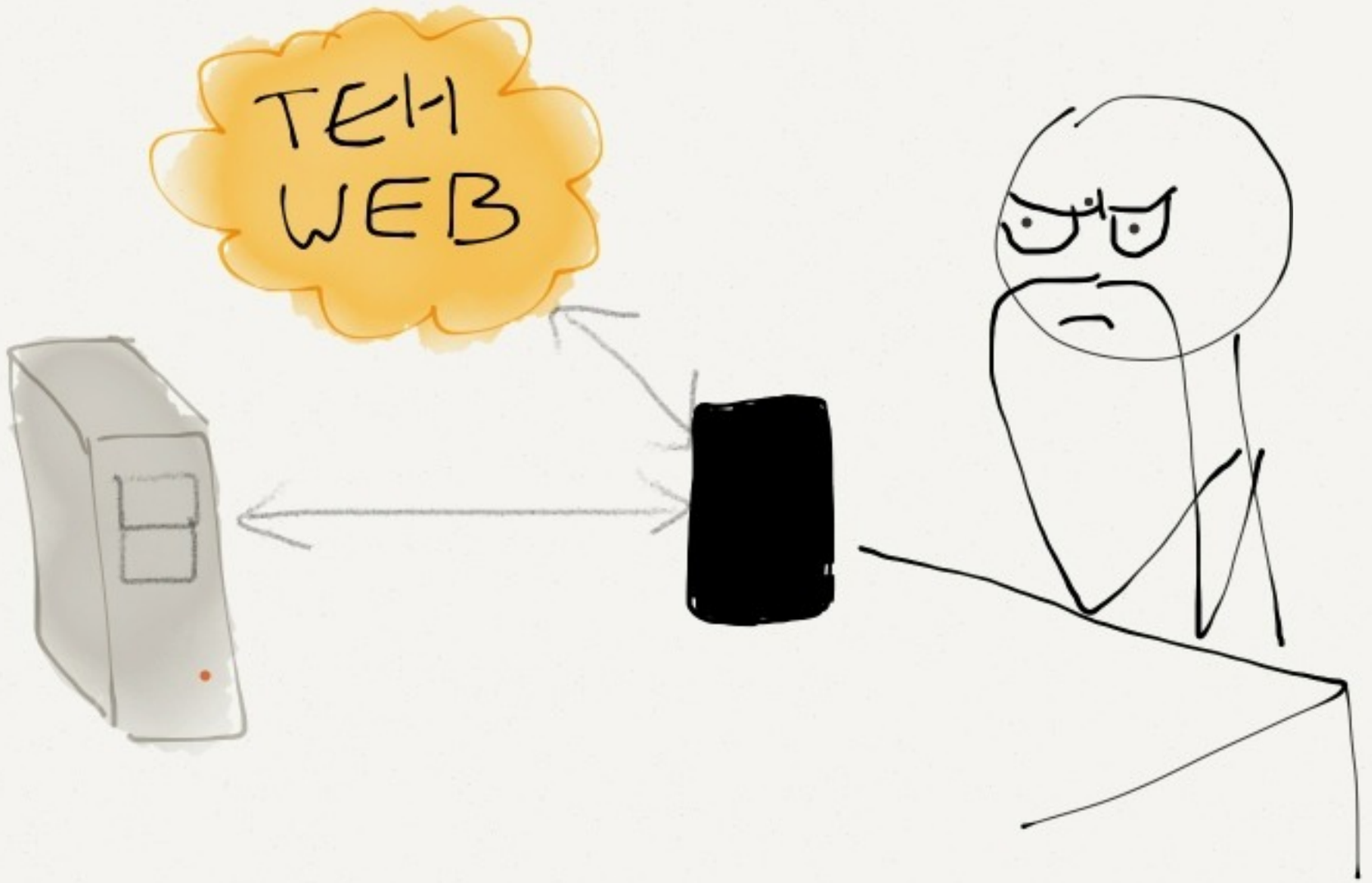
Will no-one think of the children?

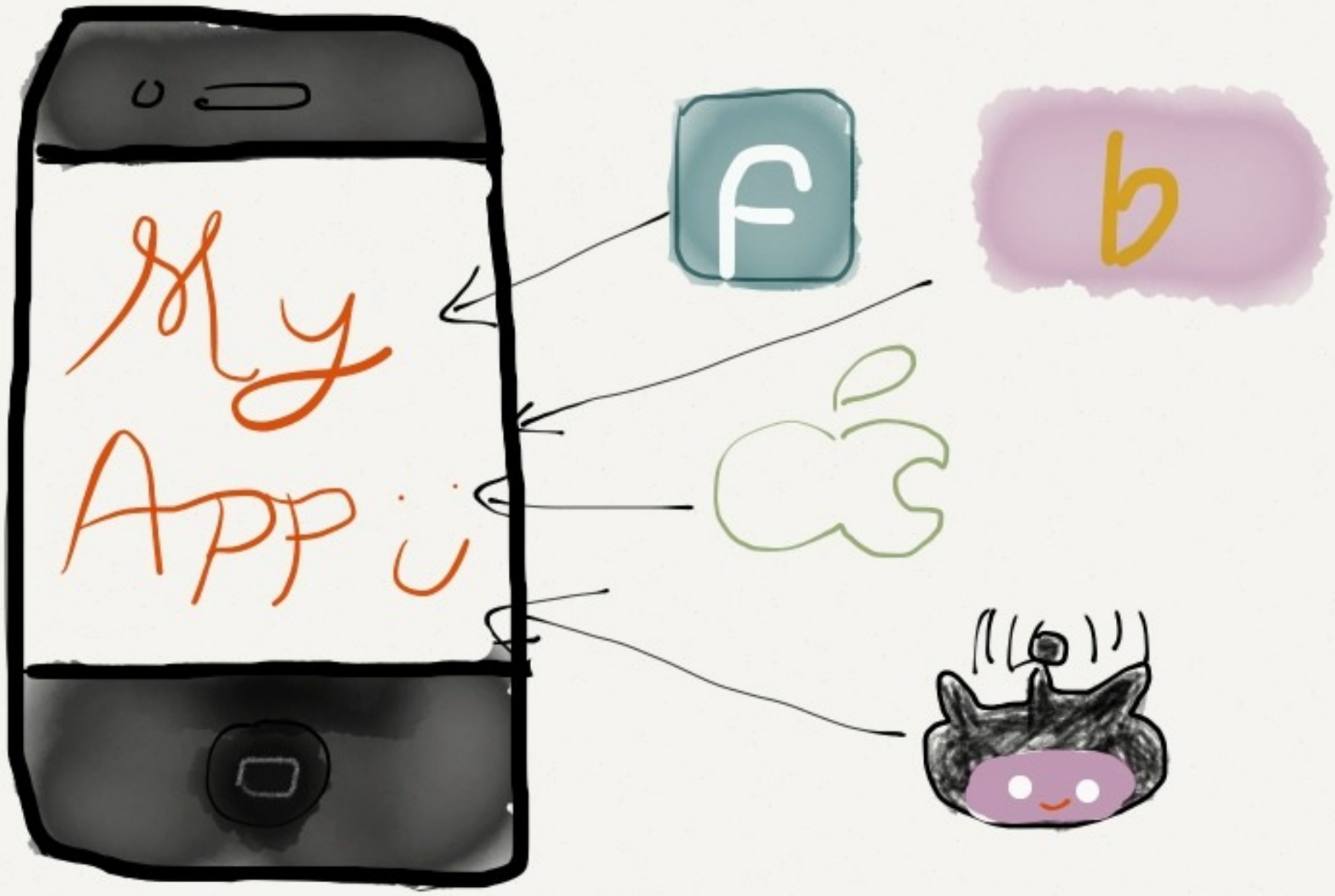


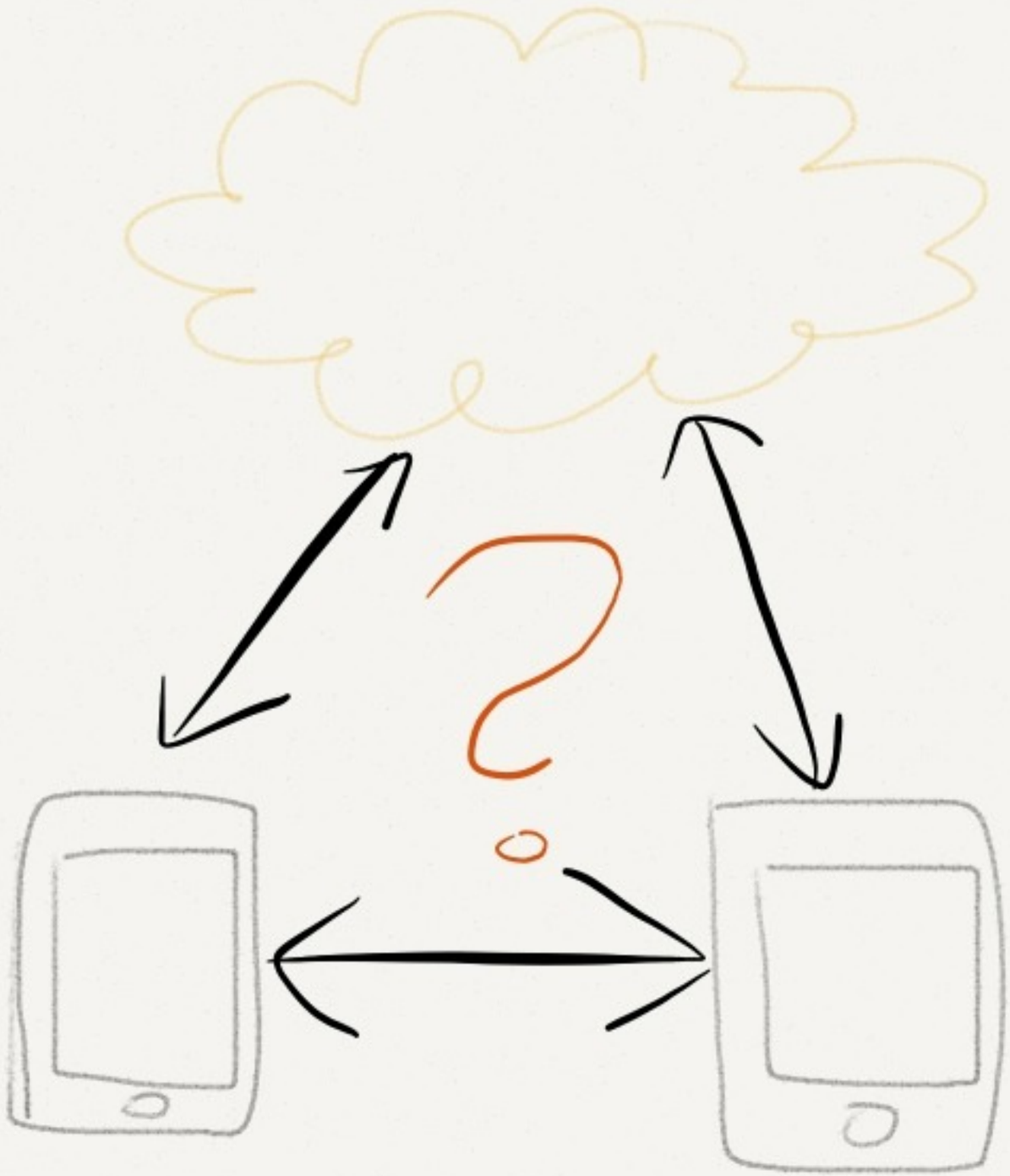
Model Your System

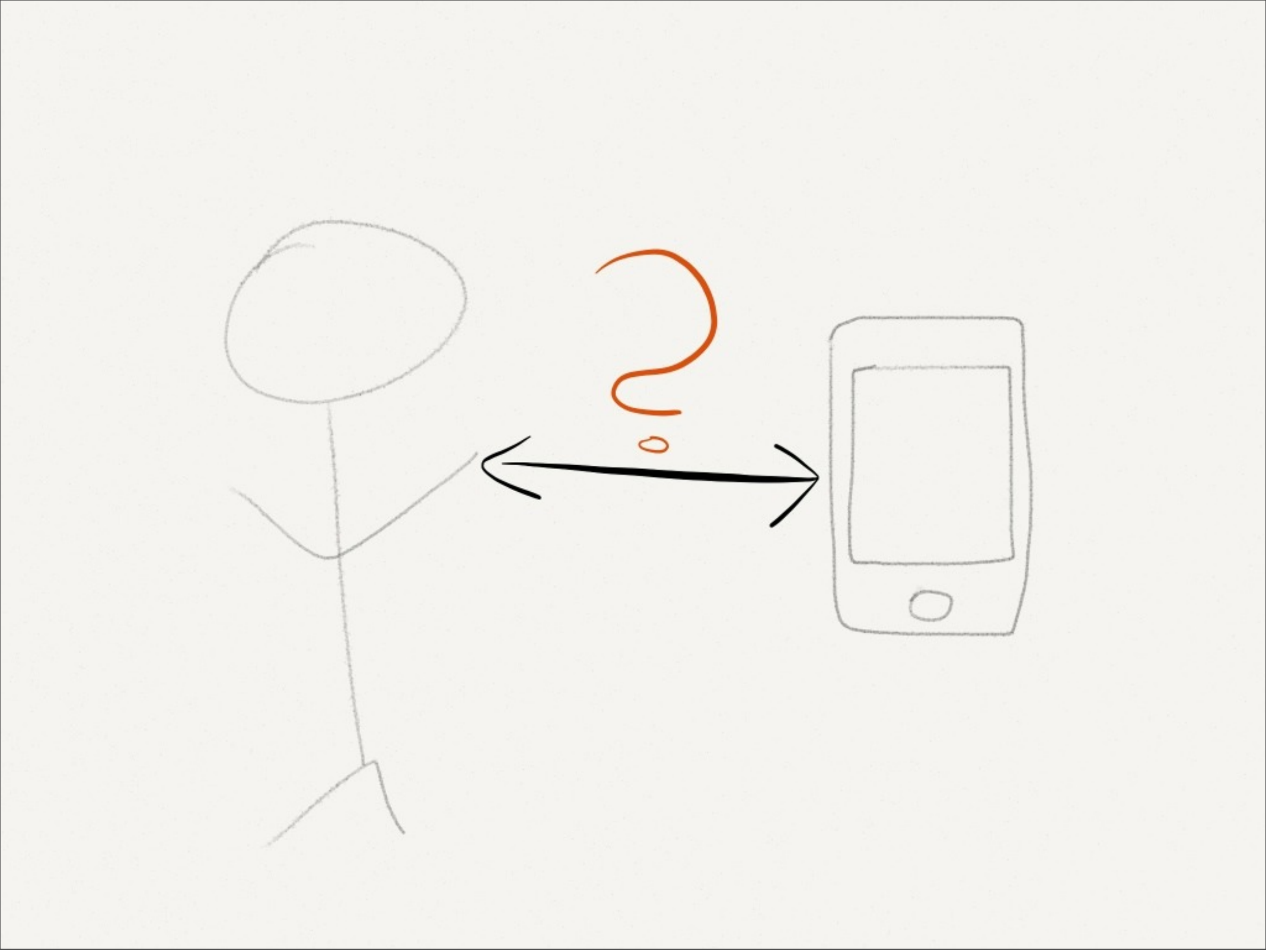


Model Your System




My
App
f
b





Top Tips

Top Tips

- Express security issues as (testable) user stories

Top Tips

- Express security issues as (testable) user stories
- Iterate

Top Tips

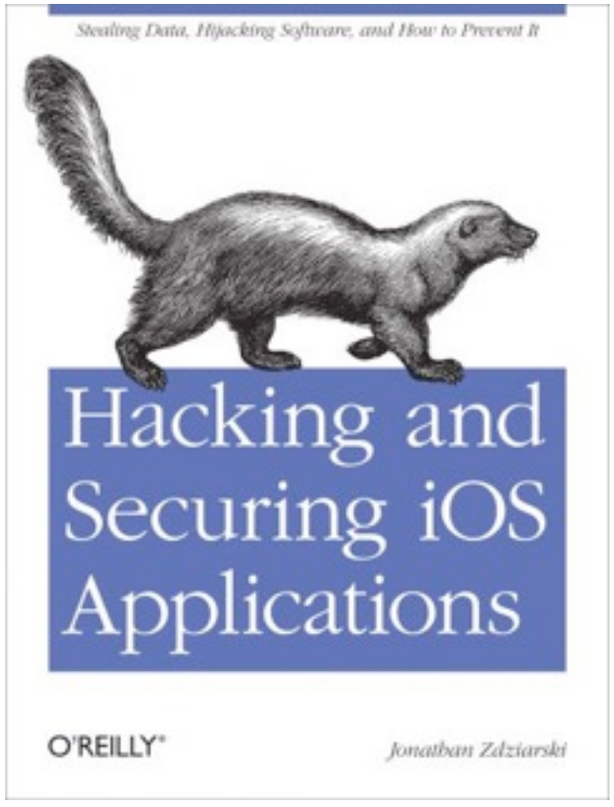
- Express security issues as (testable) user stories
- Iterate
- Plan your response strategy (particularly release management)

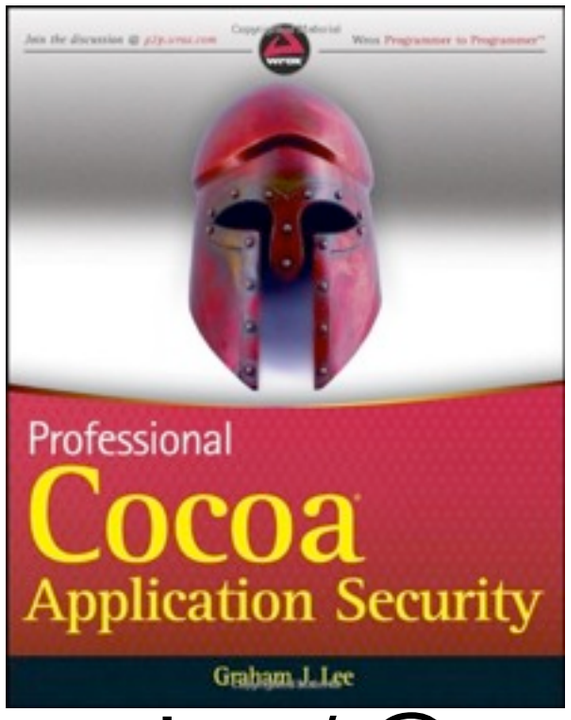
Top Tips

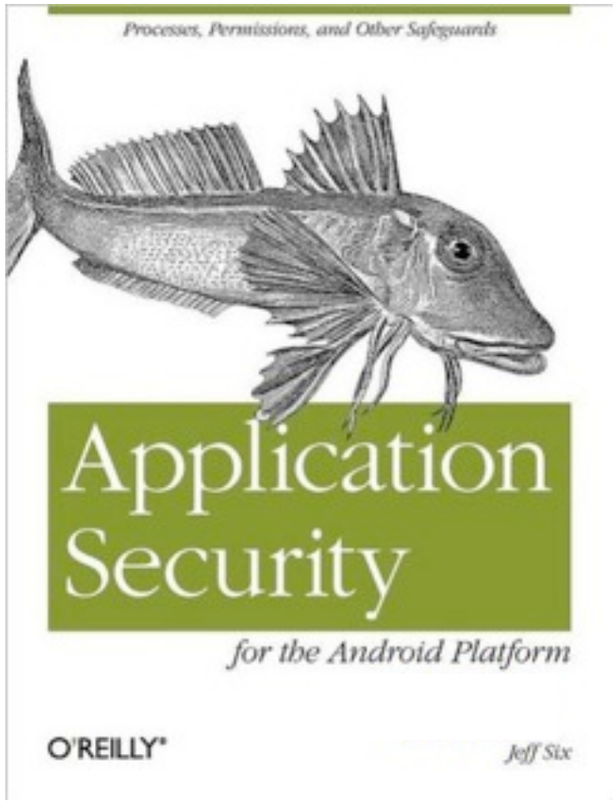
- Express security issues as (testable) user stories
- Iterate
- Plan your response strategy (particularly release management)
- Don’t leave it to the pen tester

Further Reading

- OWASP Mobile: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- GSMA Privacy Guidelines: http://www.gsma.com/publicpolicy/mobile-and-privacy/design-guidelines/







Graham Lee / @secboffin
Smartphone Security Boffin, The Lab @O2