Fraunhofer Institute for Secure Information Technology:

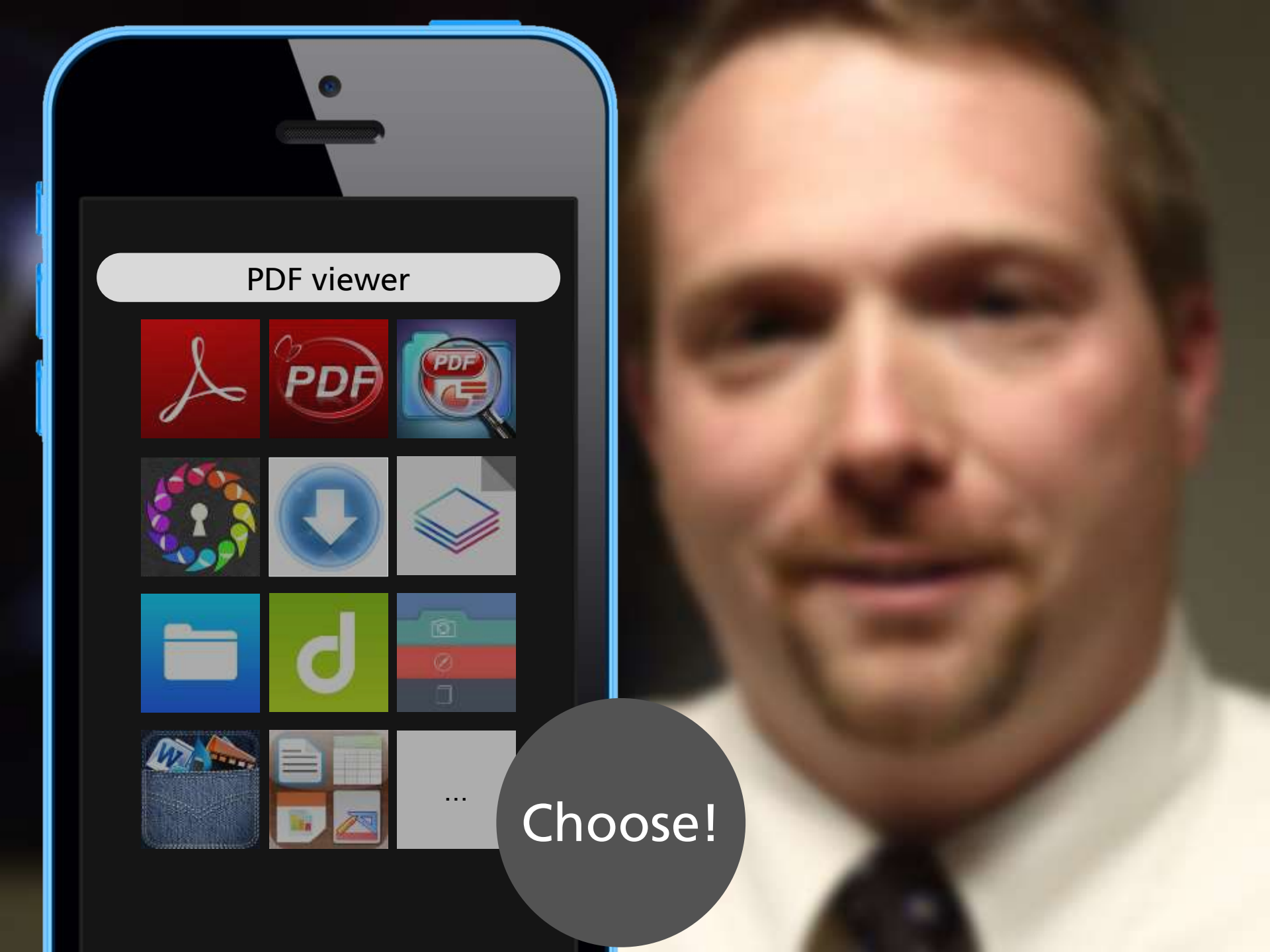
Security and Privacy for Mobile Applications

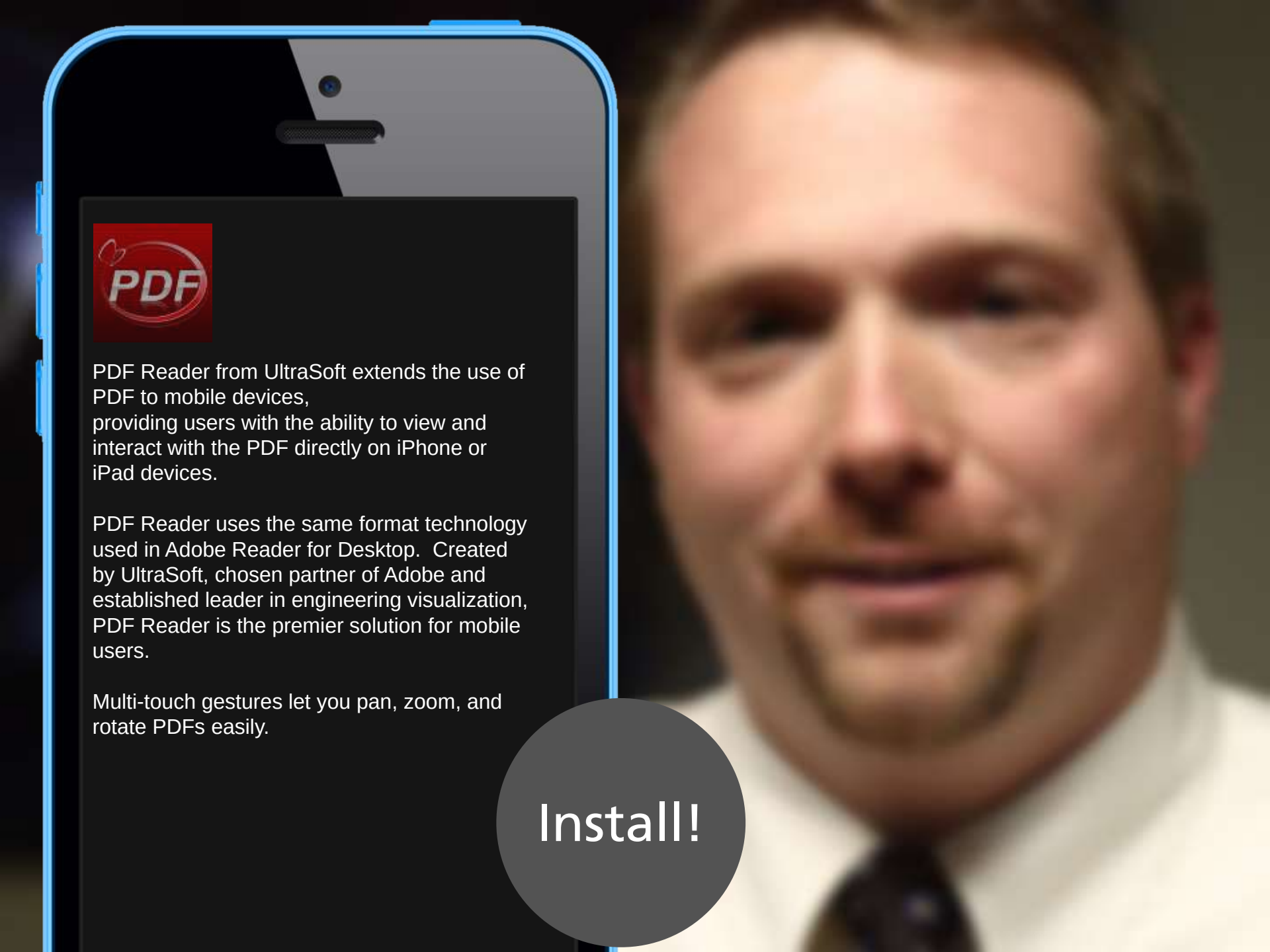
Dr. Jens Heider
Head of Department Testlab Mobile Security

CASED

Fraunhofer SIT


„I need a good PDF viewer for my iPhone!“
Dave
CEO

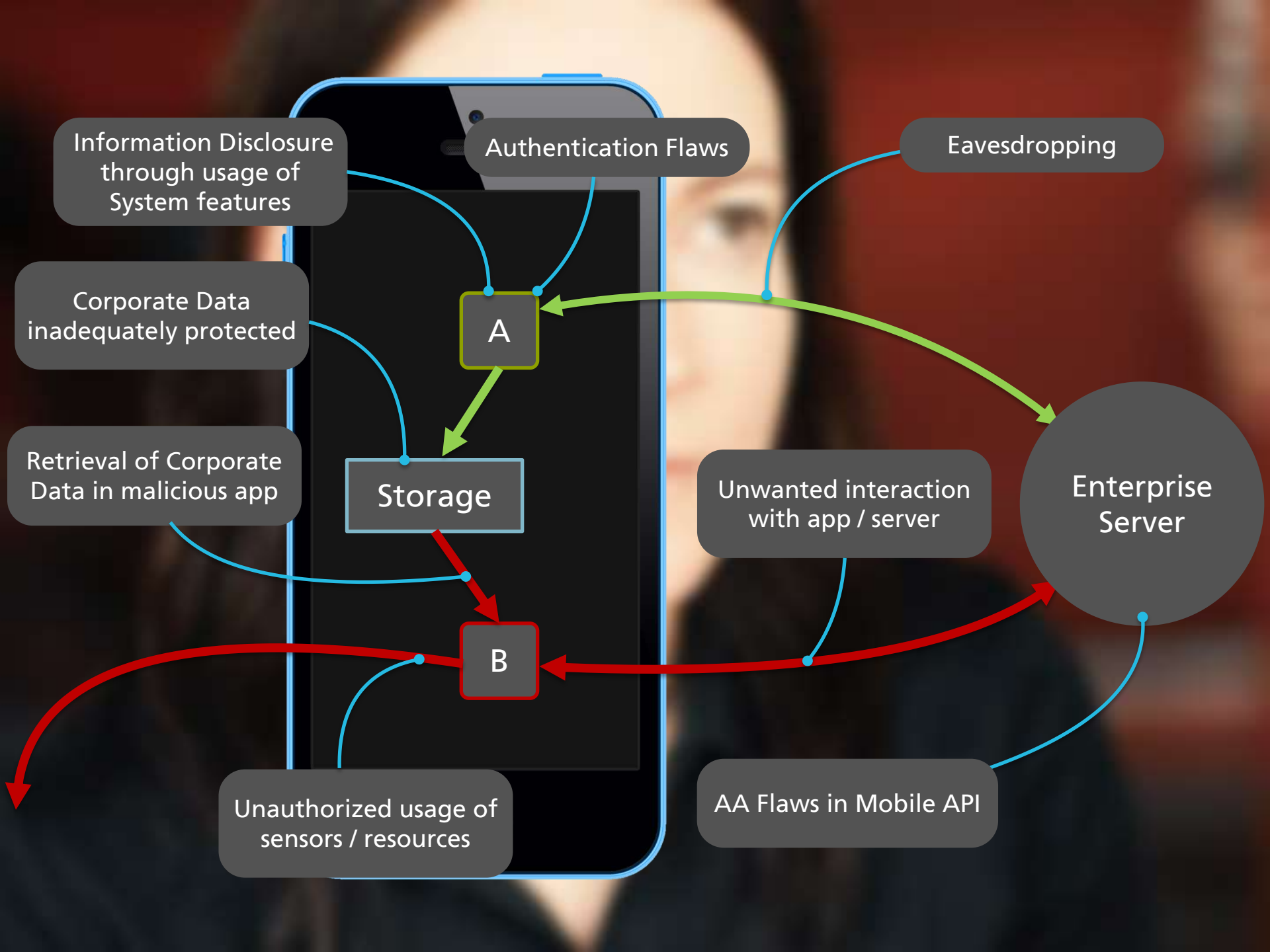

PDF viewer
PDF
PDF
...
Choose!


PDF
PDF Reader from UltraSoft extends the use of PDF to mobile devices,
providing users with the ability to view and interact with the PDF directly on iPhone or iPad devices.
PDF Reader uses the same format technology used in Adobe Reader for Desktop. Created by UltraSoft, chosen partner of Adobe and established leader in engineering visualization, PDF Reader is the premier solution for mobile users.
Multi-touch gestures let you pan, zoom, and rotate PDFs easily.
Install!

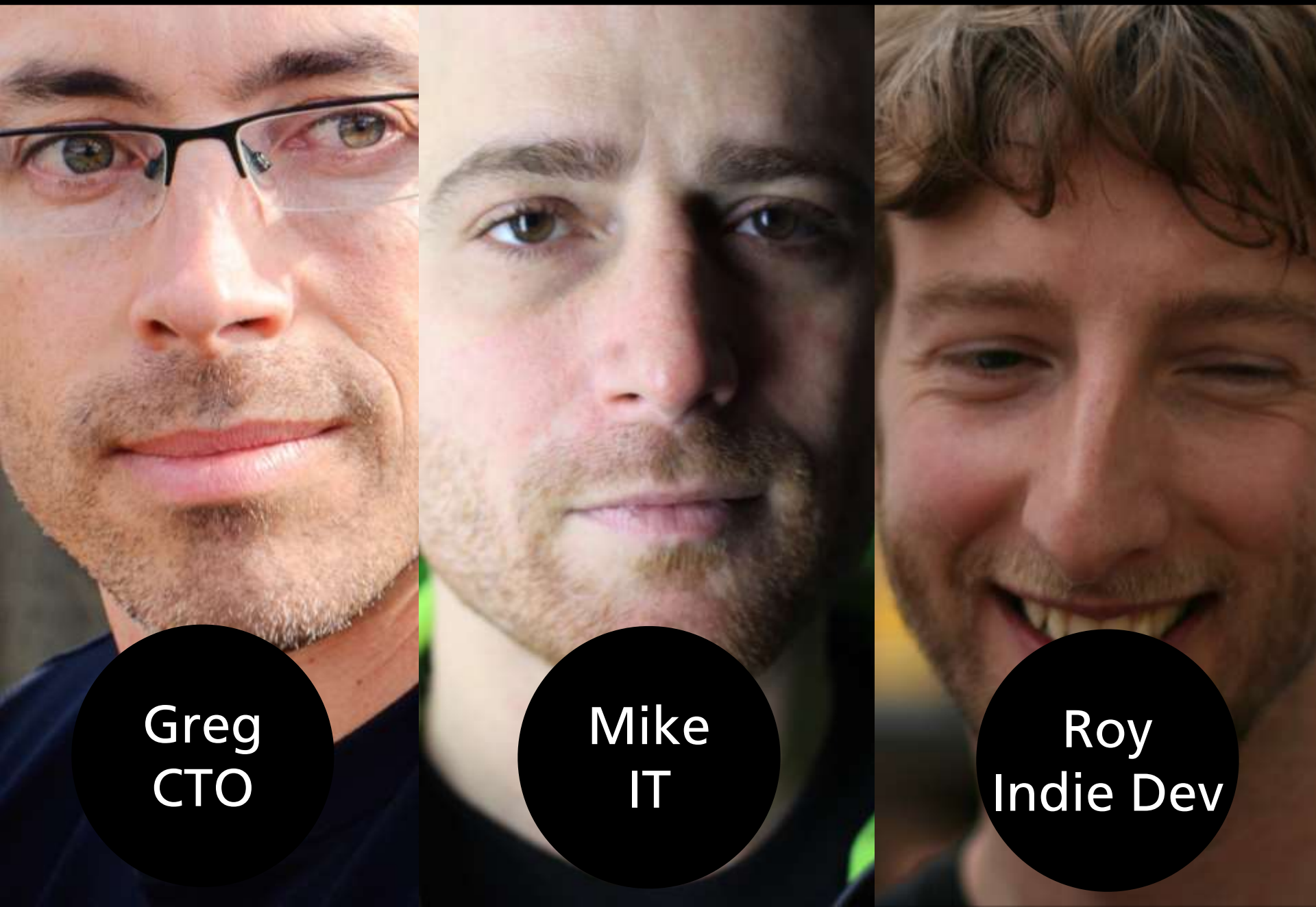

„Dave, wait! How do we know it’s security compliant?“
Kate
CSO


„Come on! it's just a PDF viewer. What can be wrong?“

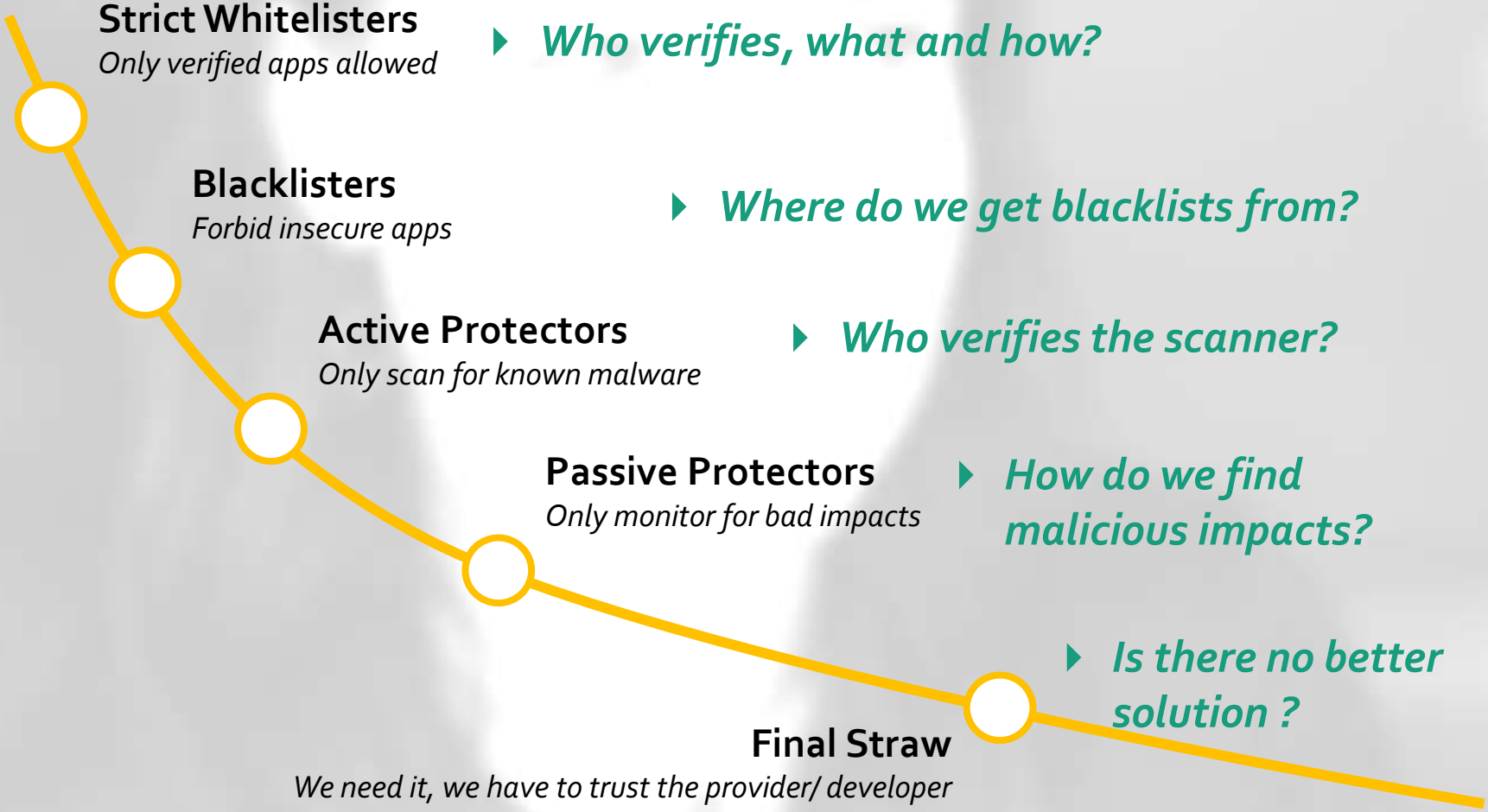

„Quite a lot“


Information Disclosure through usage of System features
Authentication Flaws
Eavesdropping
Corporate Data inadequately protected
A
Retrieval of Corporate Data in malicious app
Storage
Unwanted interaction with app / server
Enterprise Server
B
Unauthorized usage of sensors / resources
AA Flaws in Mobile API

Co-staring …

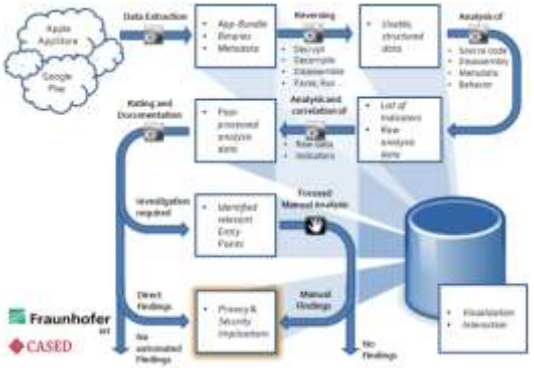


How do Enterprises deal with the App Problem?

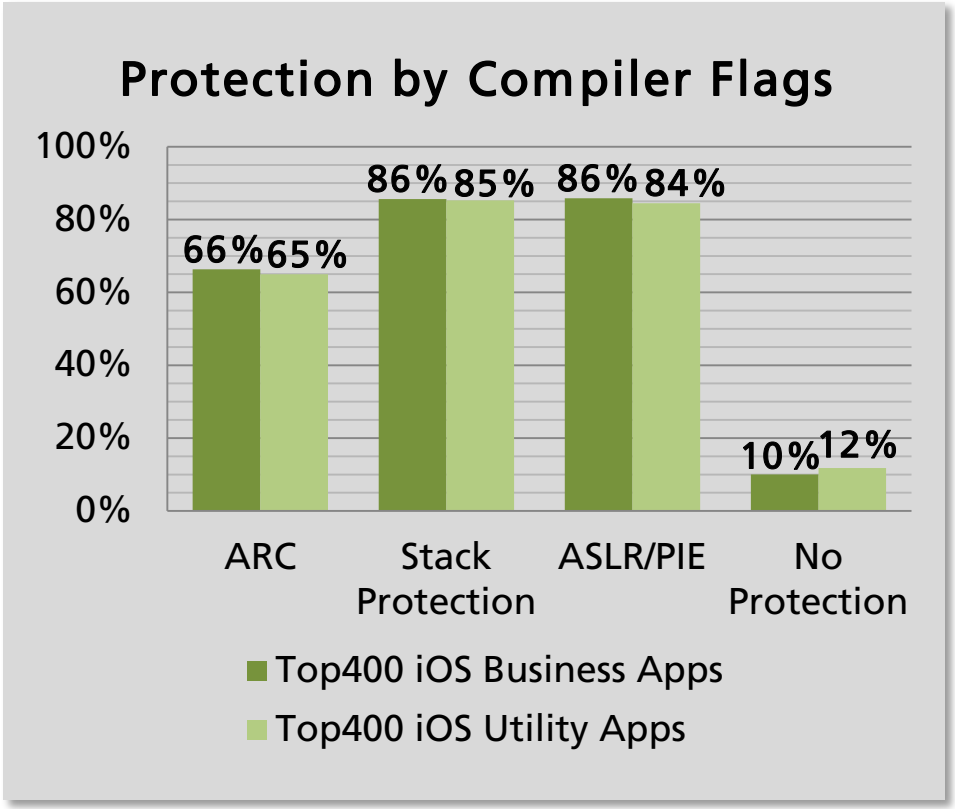


Appicaptor Framework

- Framework combining workflow and analyzing process for automated and manual app security evaluation
  - ***Distributed*** system, with simple test extensions
  - ***Dynamic*** and ***static*** code analysis
  - Scans for known ***weak/erroneous implementations*** of security functionality and ***malicious patterns***
  - Based on ***know-how*** of manual testing and integrates ***conceptual research*** of CASED
  - ***Individual report*** generation and weakness ***descriptions***
  - ***Policy-based*** recommendations for enterprise suitability



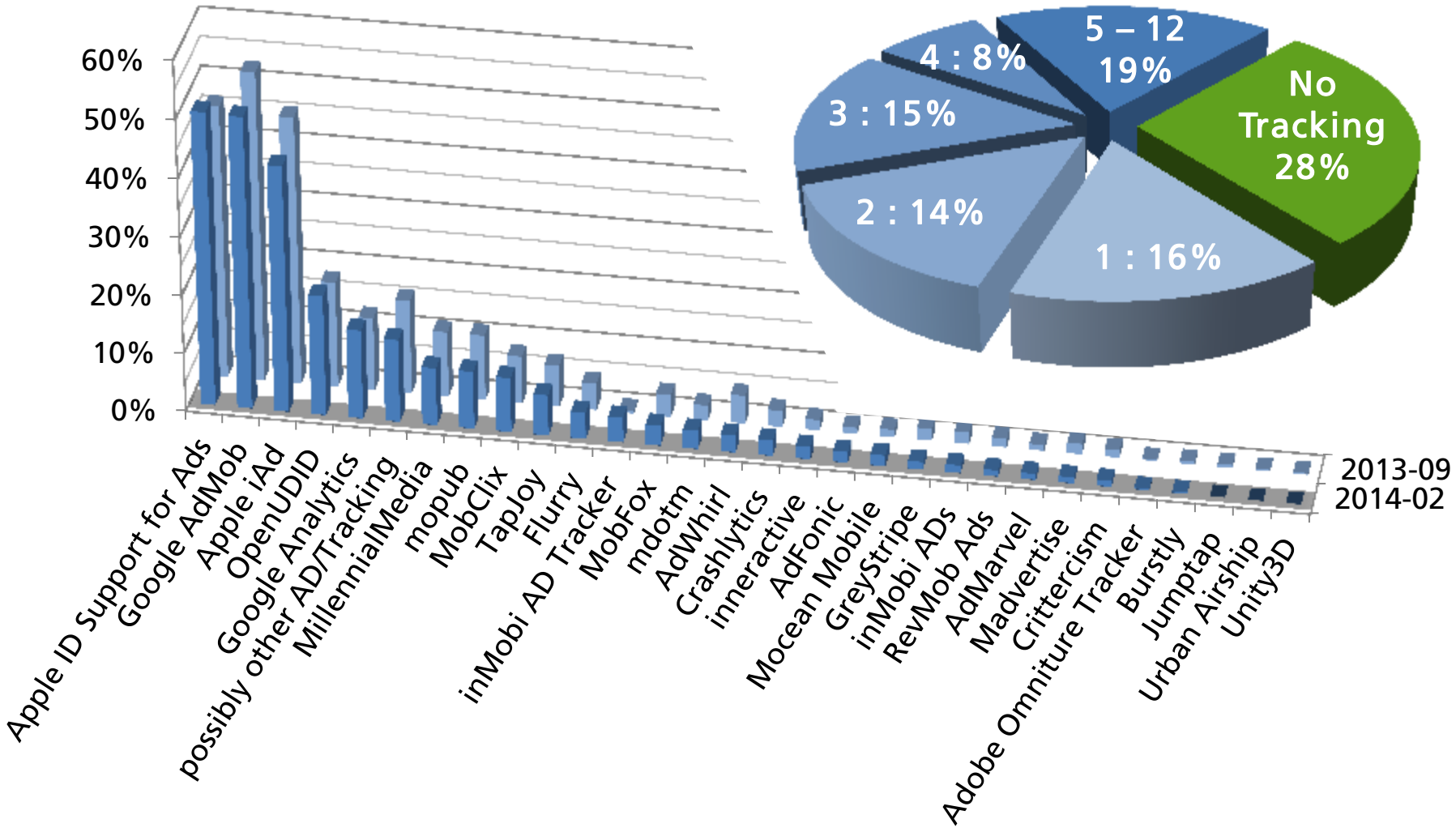
Runtime Security



Appicaptor Analysis, German App Store, 6.2.2014

- Hardening of Apps by Compiler
  - Simple to active; partly now default setting
  - **Automatic Reference Counting**: less risk for memory management flaws
  - **Stack Protection**: increase security of stack integrity
  - **Address Space Layout Randomization**: increase effort to exploit vulnerabilities
- Result of control sample
  - No significant difference between business and utility apps
  - More apps than expected have no protection

Ad- / Tracking Frameworks
Top 400 Utilities



Top iOS Apps

Appicaptor Chart Statistics
… to be published soon …

Fraunhofer SIT

CASED

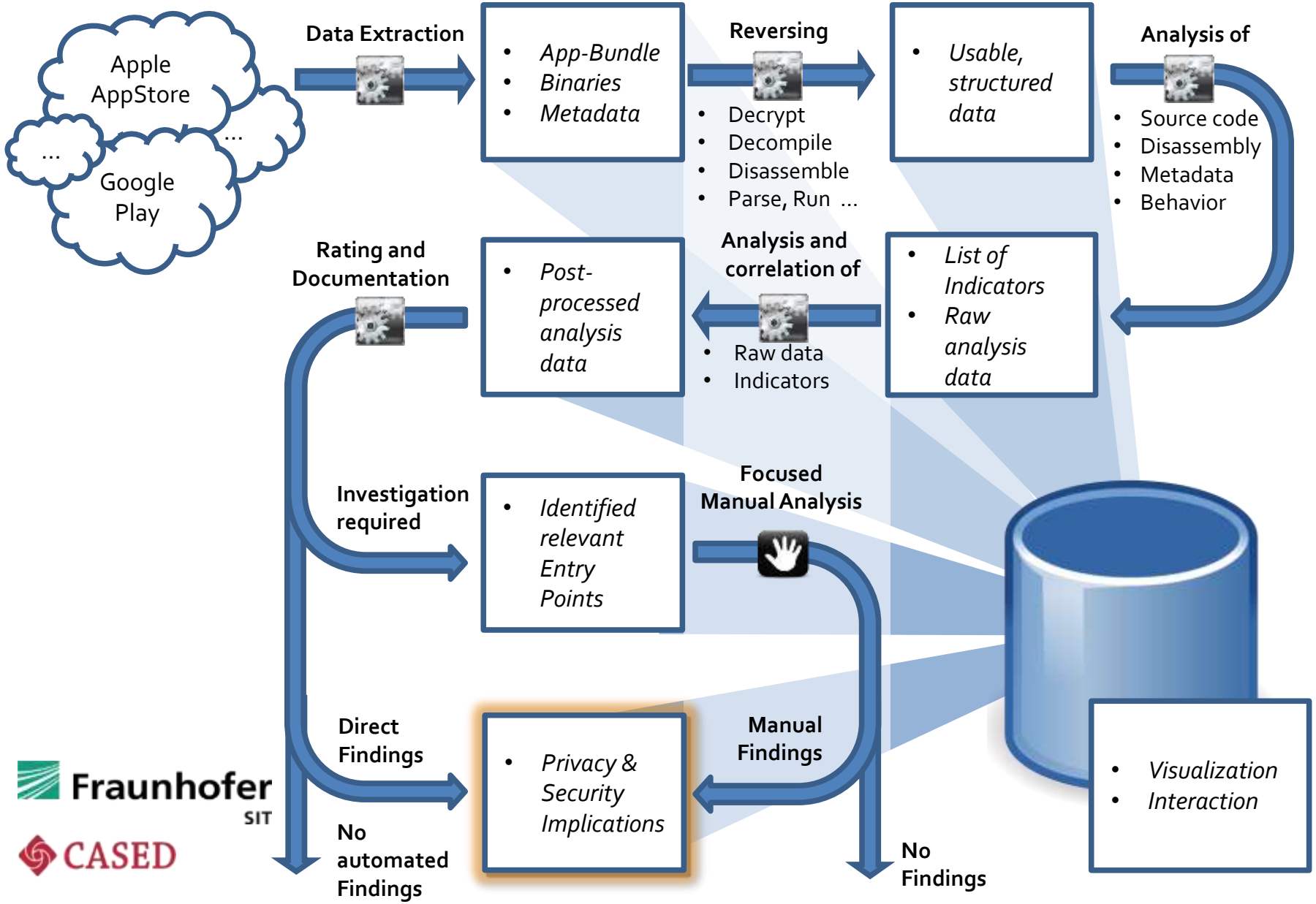
Random iOS Apps

Appicaptor Chart Statistics
… to be published soon …

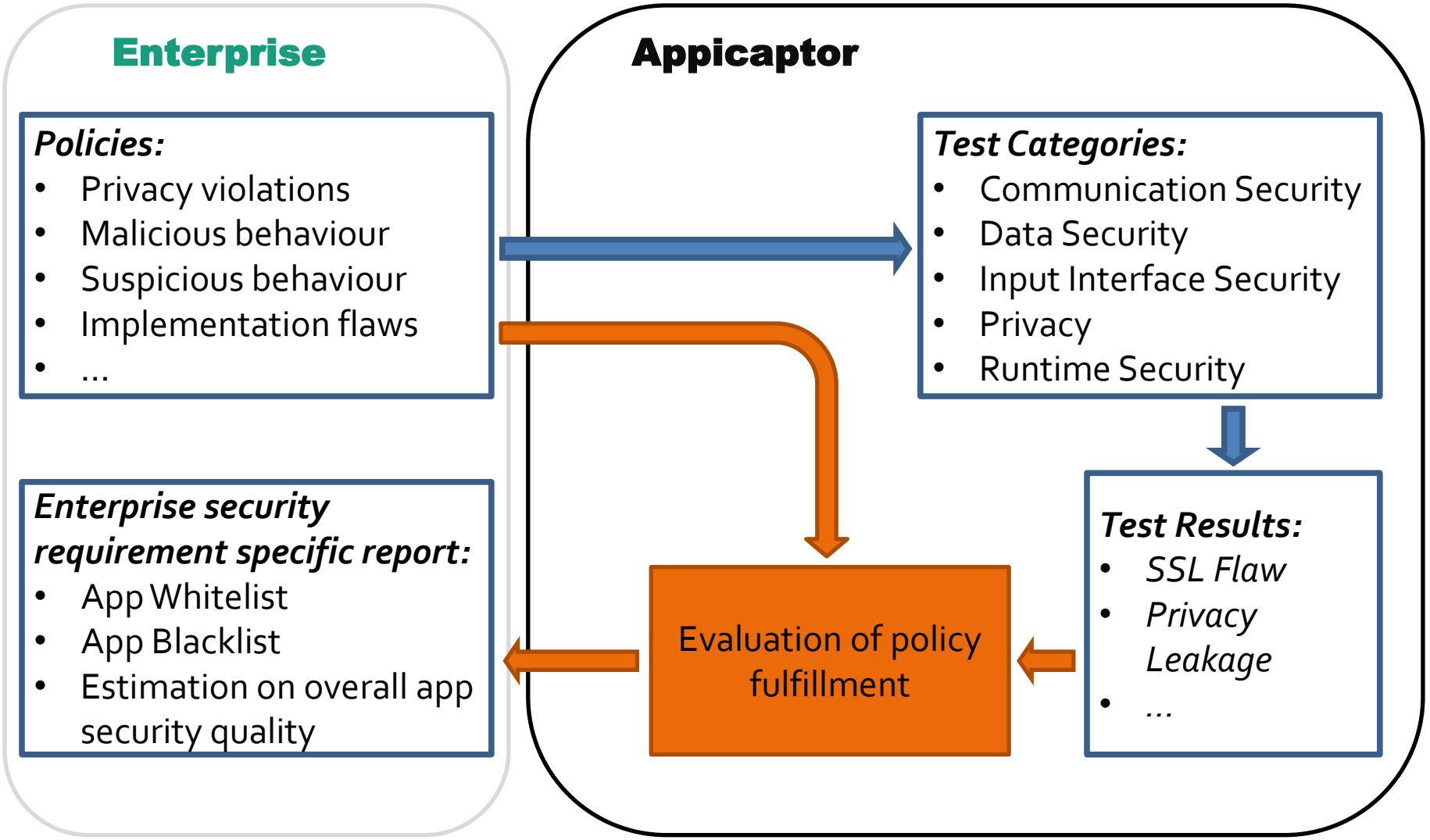
Fraunhofer SIT

CASED

Appicaptor Framework – Analysis workflow



Individual Policy Based Test Results



Appicaptor Example Report

Table 3.2: Overview of summarized test results for »ExampleXXX«

Blacklisted for enterprise usage	
☒	*Implementation flaws? Yes.*
☒	*Privacy violations? Yes.*
☒	*Security violations? Yes.*
Communication security	
☒	*Static passwords in URLs found? Yes.*
☑	*Domains accessed with http AND https:* `www.[example].net`
☐	*SSL/TLS using proper certificate validation? No.*
Data security	
☐ ⓘ	*Data protection used? No. (see details)*
☑	*Data protection classes:* `FileProtectionNone`
☐	*Keychain used? No.*
−	*Keychain classes: None*
☑	*Cryptographic Primitives:* `RC4[Enc,ECB,NoPadding],MD5`
Runtime Security	
☑	*Background activities:* `microphone`
−	*Security Compiler Flags: None.*

individual policy fulfillment evaluation

Test Results

Conclusion

- Only trusted applications should be used to handle enterprise data
- Official app markets can be a trusted source,
  but do not provide enterprise-grade security

- Define platform and application specific policies
- Automated testing processes support app baseline security
  but do not replace manual review for critical environments
- Specify platform specific security measures already in contract specification
- Keep right to use code for security audit
- White-box test more cost efficient

- Don't take security for granted. The devil is in the detail!

Contact

Dr. Jens Heider

Rheinstr. 75
64295 Darmstadt
Germany

E-Mail: jens.heider@sit.fraunhofer.de
Web: http://www.appicaptor.de
http://www.sit.fraunhofer.de

Picture Credits

IT-Guy Photo: Kris Krüg - CC BY-SA 2.0
https://www.flickr.com/photos/kk/3193513662/

CEO Photo: Sage Ross - CC BY-SA 2.0
https://www.flickr.com/photos/ragesoss/2374914189/

CSO Photo: Christopher Michel – CC BY-NC 2.0
https://www.flickr.com/photos/cmichel67/5087690757/

CTO Photo: Loren Kerns - CC BY 2.0
https://www.flickr.com/photos/lorenkerns/858692688 9/

Indie-Dev Photo: Paul Downey - CC BY 2.0
https://www.flickr.com/photos/psd/3696651661/