Fraunhofer Institute for Secure Information Technology

App Rasterfahndung: auf der Suche nach Sicherheitsqualität

Dr. Jens Heider
Head of Department Testlab Mobile Security

© Fraunhofer-Gesellschaft 2013

Requests about Smartphone Security

- How secure is iOS / Android in comparison to BlackBerry?
- How are credentials stored on iOS? Is it secure?
- We want to use MDM solution XY. How secure is it?
- Is it possible to integrate iOS securely in our existing network (e.g. VPN)?
- How secure is App XY? Does it store data securely?
- We are developing an App for iOS / Android. How secure is our concept and implementation?

Platform Security Testing

Network Security Testing

Application Security Testing

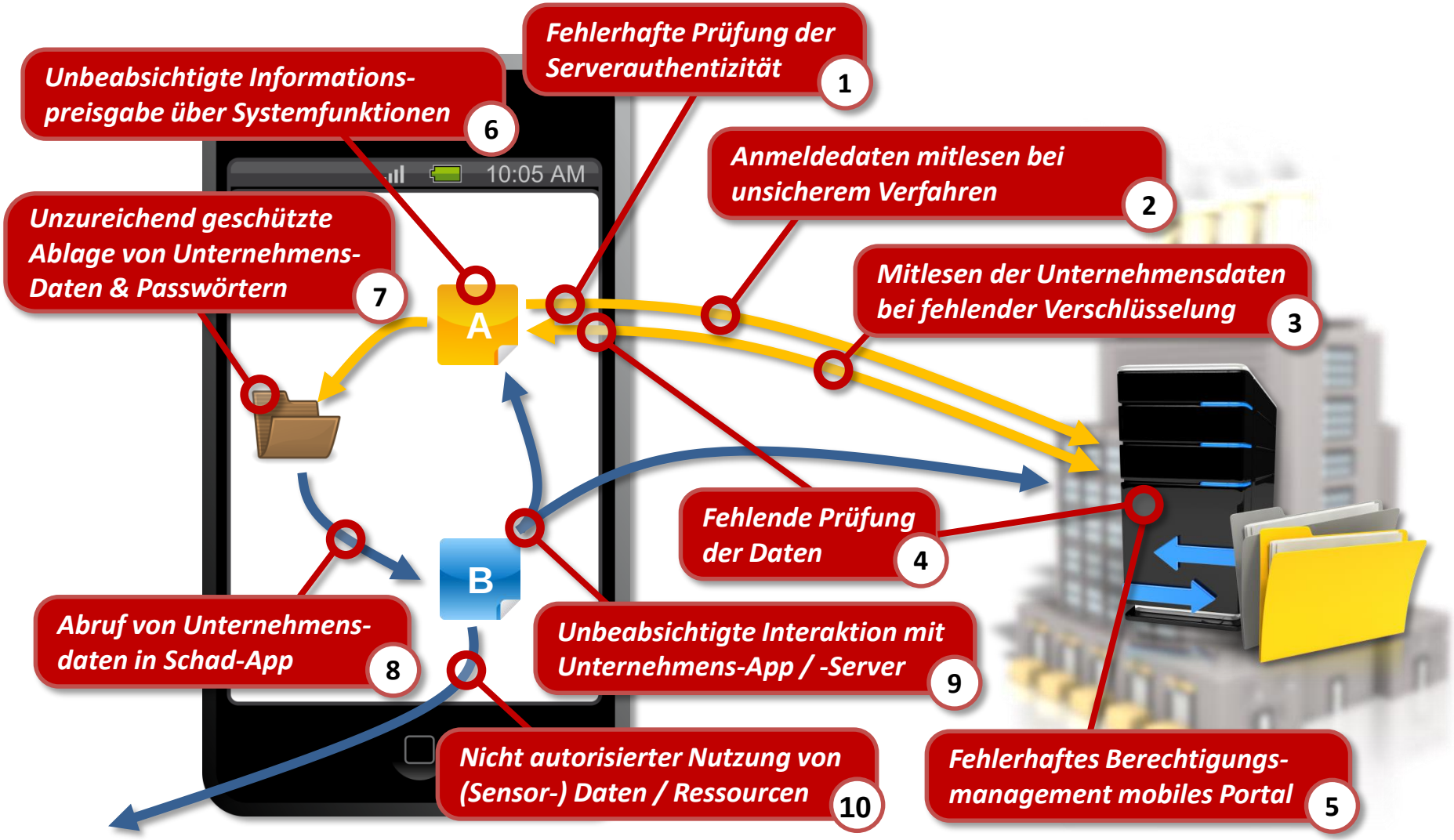
© Fraunhofer-Gesellschaft 2013

The App Problem

Q4 / 2012

© Fraunhofer-Gesellschaft 2013

Verwundbarkeiten von Unternehmens-Apps



How does Enterprises deal with App Protection?

Strict Whitelisters
Only verified apps allowed

- *Who verifies, what and how?*

Blacklisters
Forbid insecure apps

- *Where do they get blacklists from?*

Active Protectors
Only scan for known malware

- *Who verifies the scanner?*

Passive Protectors
Only monitor for bad impacts

- *How do they find malicious impacts?*

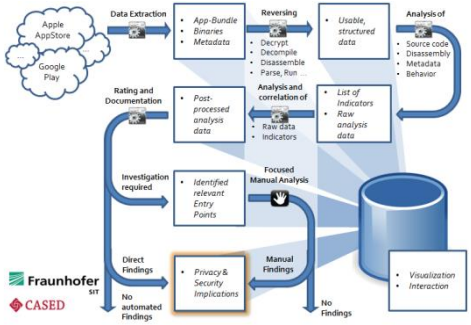
- *Why are there no promising solutions?*

Those how have already surrendered
The users need it, we can't stop them

© Fraunhofer-Gesellschaft 2013

Appicaptor Framework

- ***Framework accumulates workflow and analysis tools for automated and manual app security evaluation***
  - Scans for known ***malware patterns*** and ***weak implementations*** of security functionality
  - Smartphone ***Platform agnostic*** and correlates platform results
  - Based on ***knowhow*** of manual testing and integrates ***conceptual research*** of CASED
  - Workbench visualizes ***interpreted results*** and ***entry points*** for manual investigations



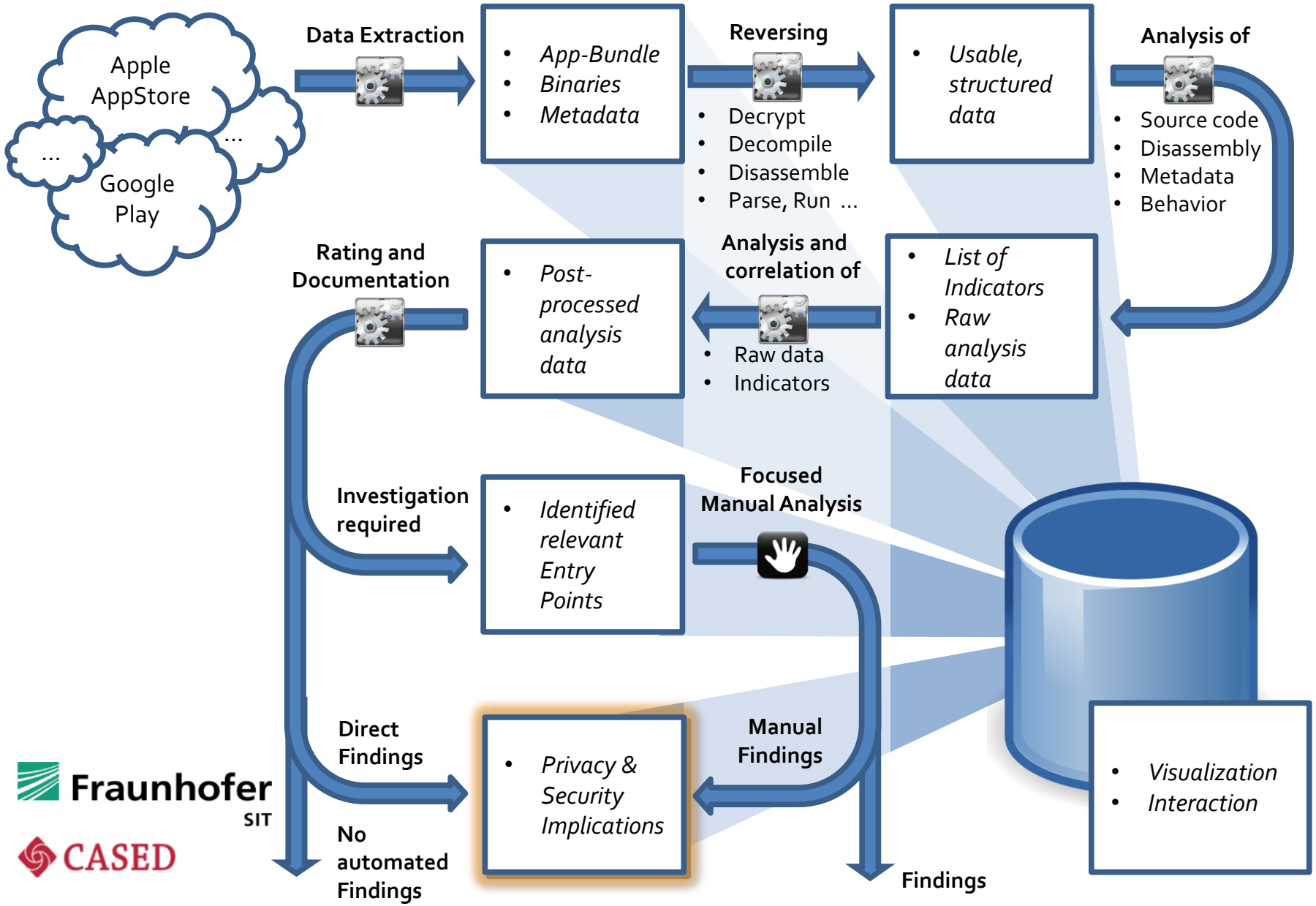
„ Investment in your Future "

HESSEN

Investments for this work were co-funded by the European Union
with European regional development funds
and by the state government of Hessen

© Fraunhofer-Gesellschaft 2013

SIT Appicaptor Framework – Analysis workflow



Example: Insecure SSL usage

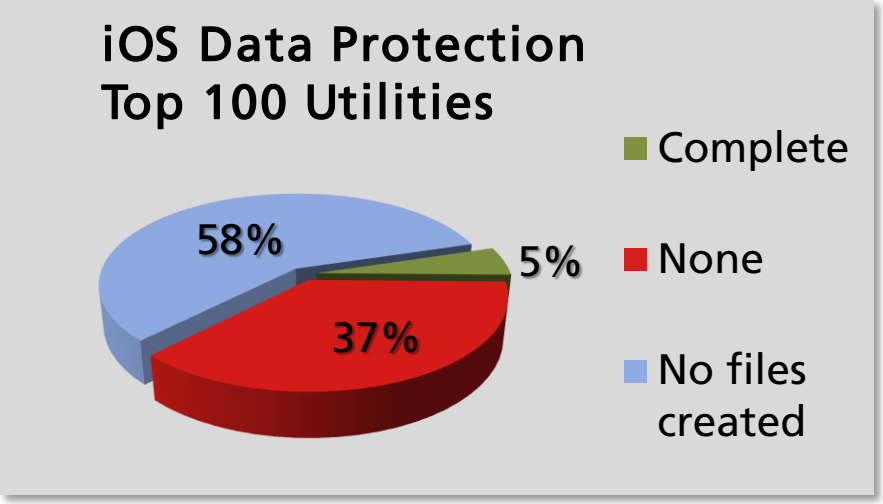
- Problem e.g.:
  - Missing or incomplete certificate validation
  - Self signed certificate for back end systems
- Detecting:
  - Static: call graphs of identified API functions
    (e.g. is *cancel()* in path of implemented or overwritten API functions?)
  - Correlated with dynamic tests with crafted certificate pool

In the wild Android example: Smali representation of insecure certificate validation in banking app

```
.method public onReceivedSslError
(Landroid/webkit/WebView;Landroid/webkit/SslErrorHandler;Landroid/net/http/SslError;)V
.locals 0
.parameter "iwv"
.parameter "sslh"
.parameter "ssle"
.prologue
.line 118
invoke-virtual {p2}, Landroid/webkit/SslErrorHandler;->proceed()V
.line 119
return-void
.end method
```

© Fraunhofer-Gesellschaft 2013

Example: Missing protection of Stored Data

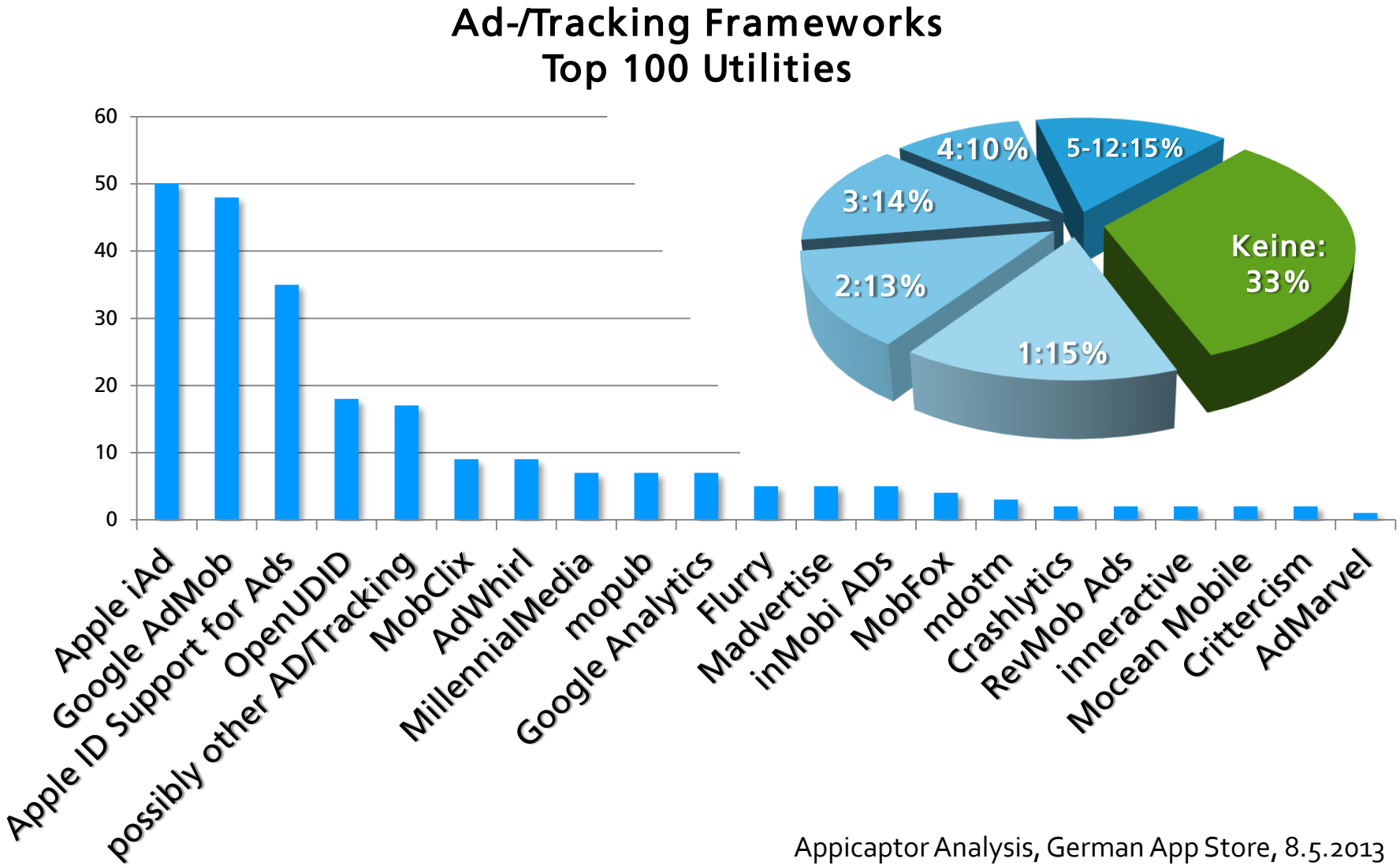


Appicaptor Analysis, German App Store, 8.5.2013

- iOS functionality to keep files encrypted in storage
  - Incorporates passcode as user secret for encryption + bruteforce protection
  - Protection for lost/stolen devices
  - Rarely used by system apps
- Result of control sample
  - Also rarely used in analyzed 3rd party apps
  - Of 8 apps with office file support, only 2 use data protection

© Fraunhofer-Gesellschaft 2013

Example: unexpected Functionality



Appicaptor Analysis, German App Store, 8.5.2013

© Fraunhofer-Gesellschaft 2013

Conclusion

- ***Control over used software***
  - Same as desktop software: only trusted software should be used with enterprise data
- ***Inspection***
  - Official app markets trusted source,
    but does not provide security quality for enterprises
  - First preliminary results of automated scan indicate flaws known from manual testing
  - Framework provides possibility to integrate known analysis methods to focus on test cases
- ***Impact***
  - Making app security quality a criteria for enterprises necessary for Mobile Device Management

© Fraunhofer-Gesellschaft 2013

Contact

Dr. Jens Heider

Rheinstr. 75
64295 Darmstadt
Germany

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

© Fraunhofer-Gesellschaft 2013