TeleTrusT T.I.S.P. Community Meeting

Berlin, 14./15.11.2017

App-Härtung ist für Ihre mobile Strategie entscheidend

Matthias Reichert, Promon AS

Unfortunately: many apps in many segments offer essentially no resistance to attack by common and easy to use attack-methods…

Video - How a Tesla was stolen by hacking the app

https://www.youtube.com/watch?v=5jQAX4540hA

https://www.youtube.com/watch?v=S7lCw7YDddg

Background

- According to TrendMicro: nearly 90 percent of Android devices are exposed to at least one critical vulnerability, because of Android handset makers' failure to deliver patches.
  http://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices/

- According to a recent study: mobile users are massively unaware of cyber threats, with an overwhelming 89 percent of respondents admitting they wouldn't know if their device has been infected through a cyber attack.

Trend – Fake and infected apps in official stores

"Google decides to remove millions of apps from Play Store"

Source; http://www.gizbot.com/apps/news/google-will-remove-millions-apps-from-play-store-march-15-038194.html

"Apple is still struggling to keep fake apps out of the App Store"

Source; http://uk.businessinsider.com/apple-still-struggling-to-keep-fake-apps-out-of-the-app-store-2016-11?international=true&r=UK&IR=T

Leading AV vendor, completely acknowledges our approach

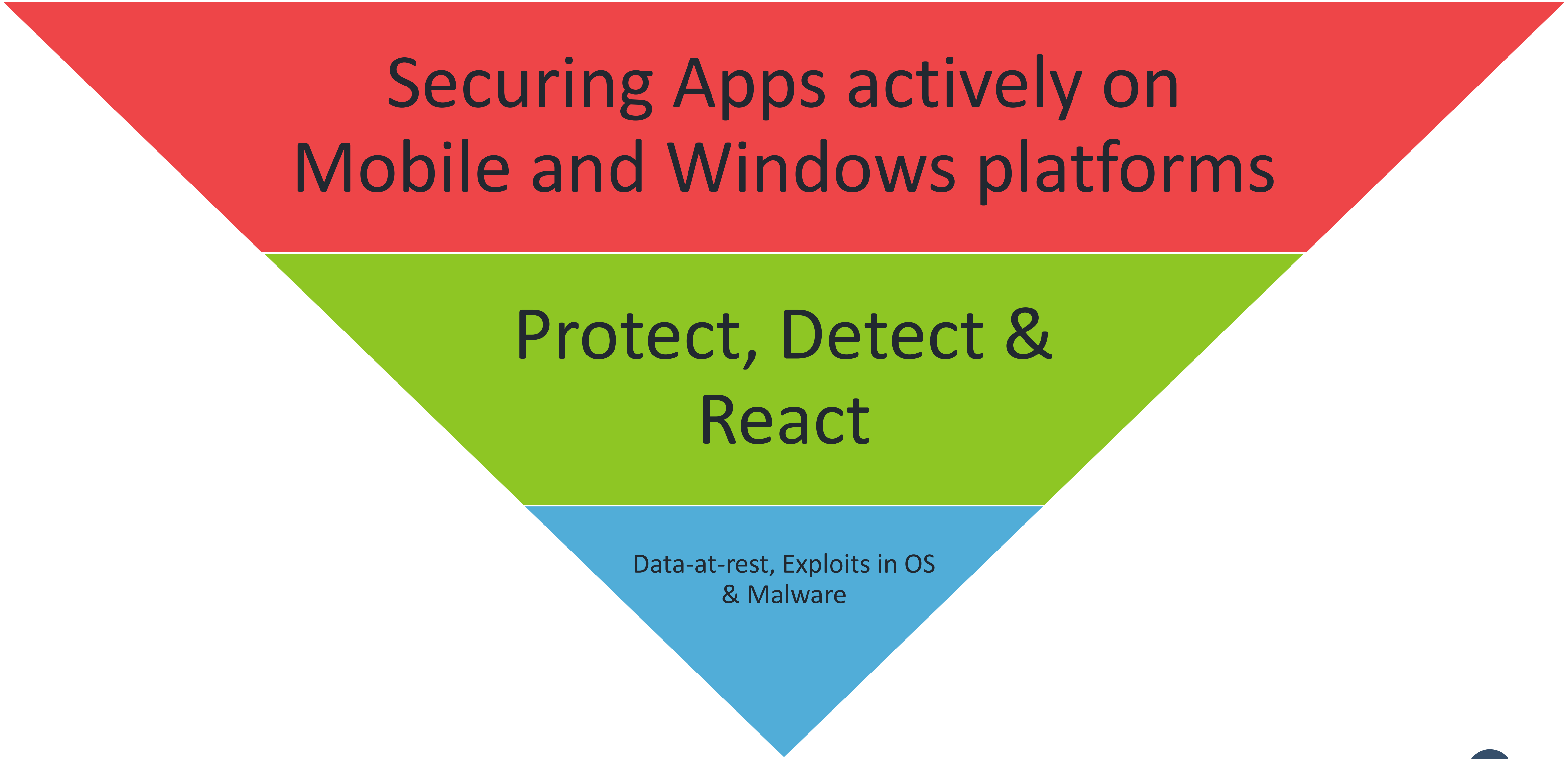
"In the mobile world, it is really about application shielding – application hardening."

Raimund Genes
Trend Micro CTO – CeBit 2017

Rock-Solid App Security

This is App Security

What you must do – top down

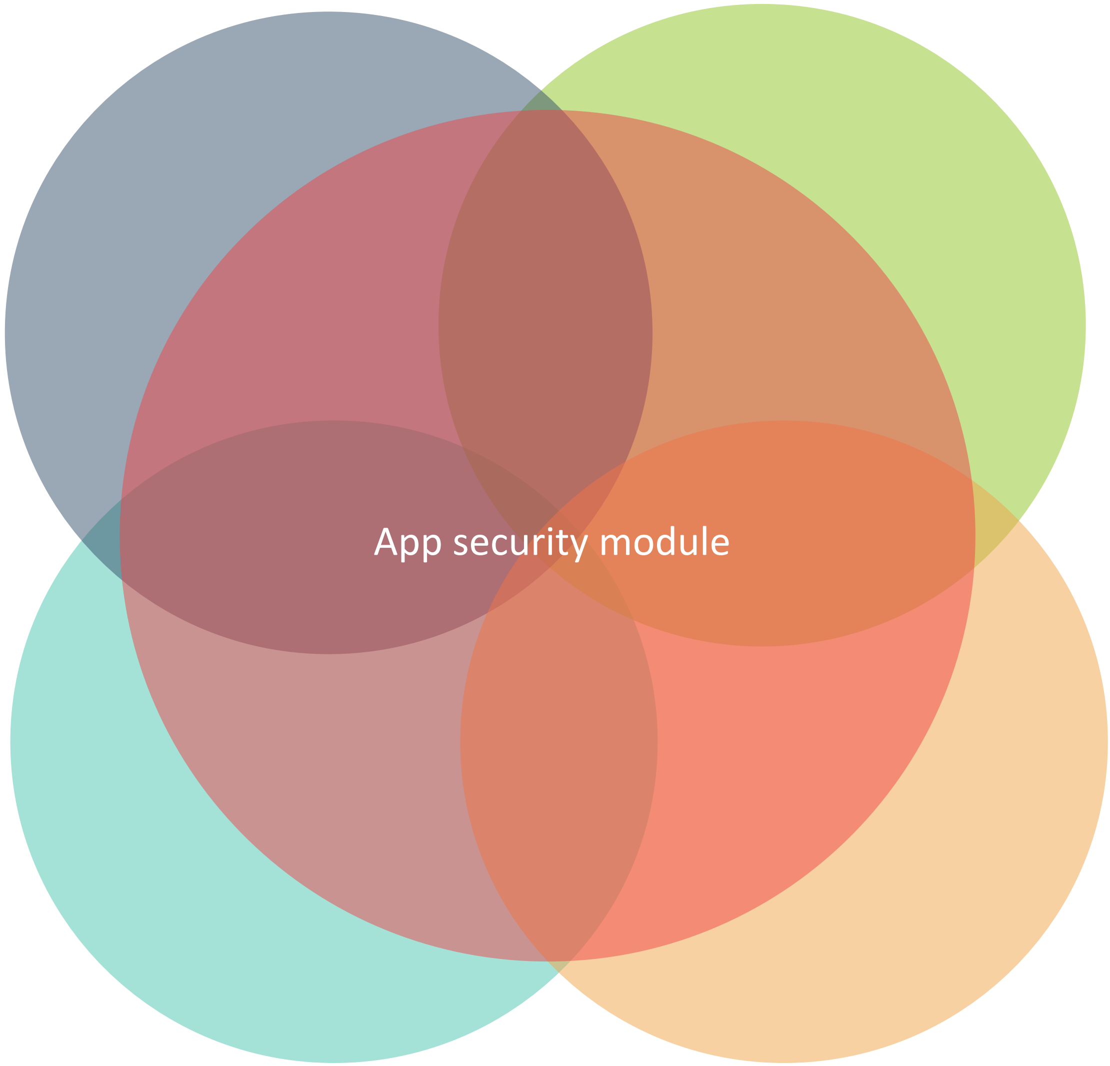


Securing Apps actively on Mobile and Windows platforms

Protect, Detect & React

Data-at-rest, Exploits in OS & Malware

In the sweet spot



Runtime Application
Self-Protection (RASP)

App hardening

At Runtime

App security module

At Rest

Fraud detection

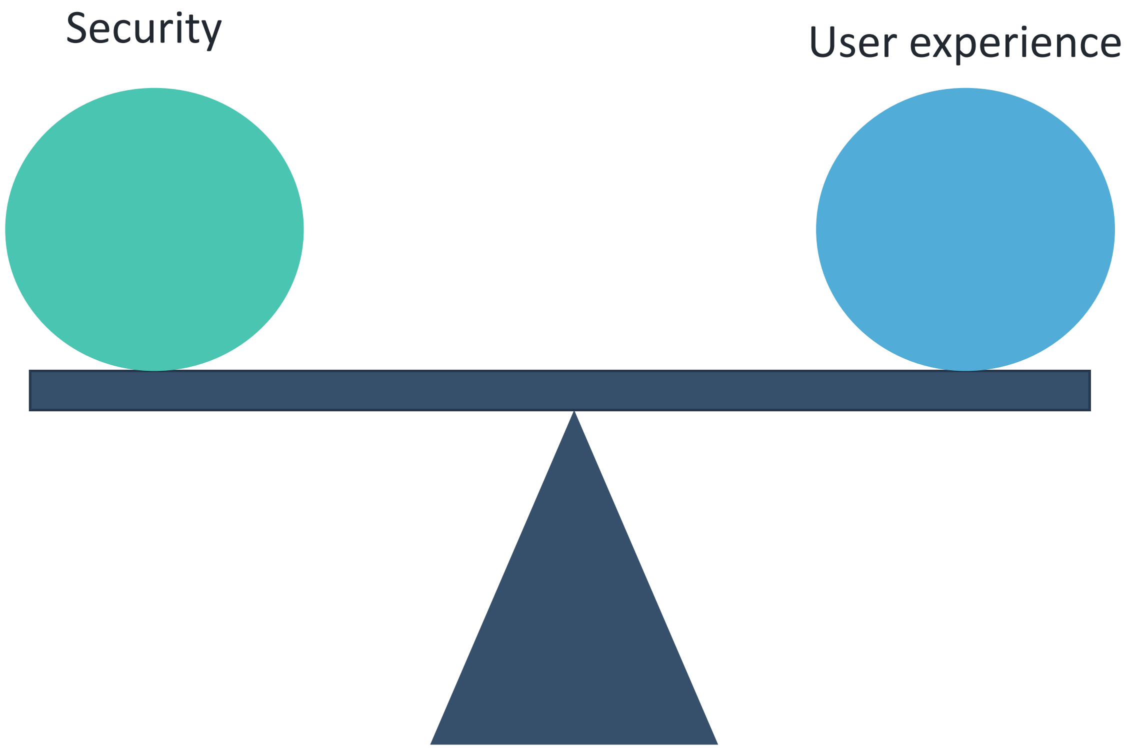
Obfuscation

Tech Concepts

- Proactive & whitelist based
- Integrated security (app binding)
- Self-contained
- Multi-layered
- Block, detect, report (visibility)
- ‘Under the hood’ - Low level monitoring & control of the complete execution environment of the app

Tech Strategy

- Client Apps – Integrated Security
- Unified High Level of Security – Cross platform
- Maximise Security – **Without** negative impact on end-user experience
- Maximise Security – with Easy/Automated integration (integration/developer convenience)



What can the app providers do

What Tesla could have done better

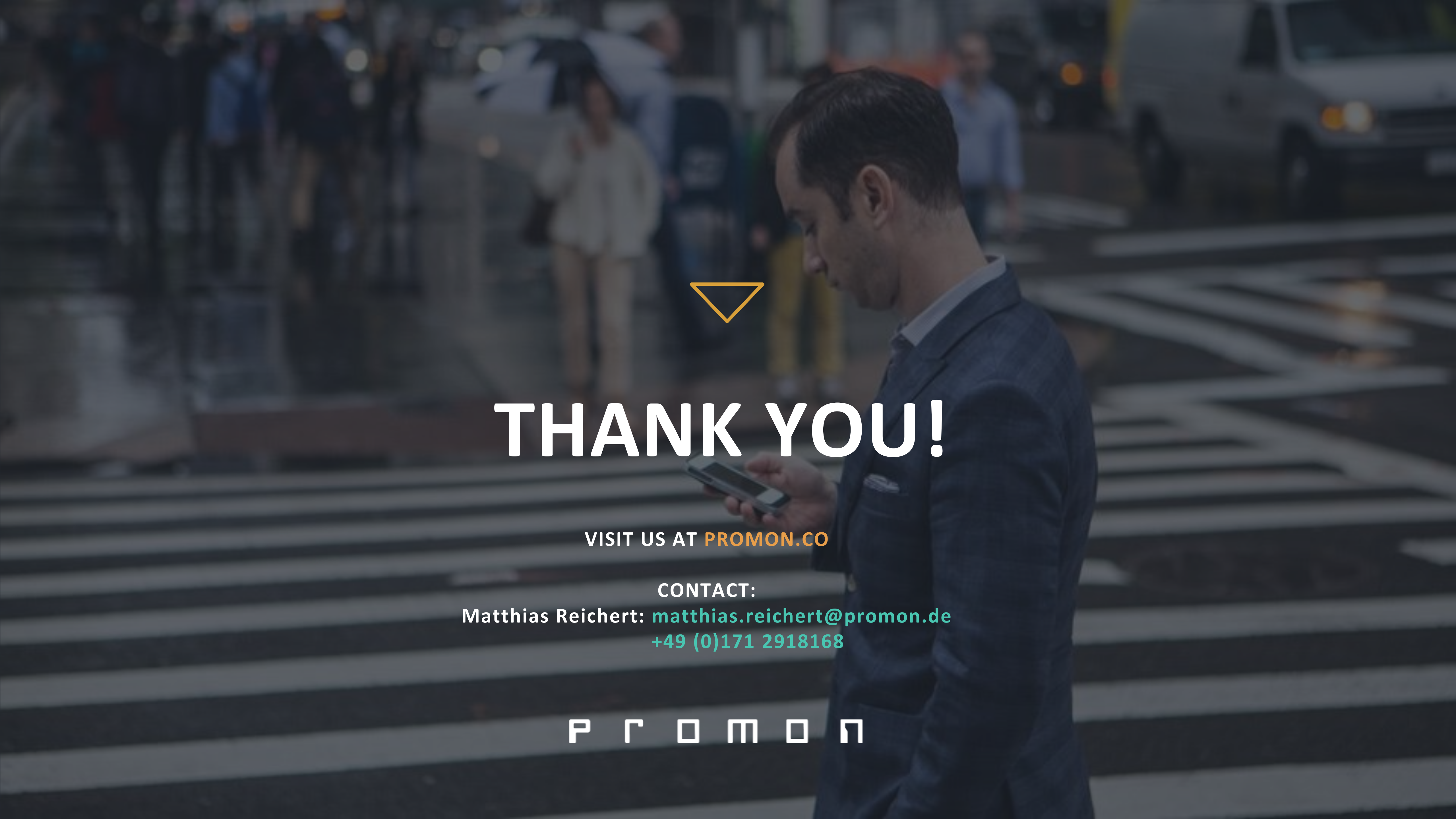
What can app providers learn from this?

- The app should detect that it has been modified.
- The authentication token should not be stored in clear text.
- The security of the authentication can be improved by requiring two-factor authentication.
- The app should provide its own keyboard for entering the username and password. Otherwise, malicious third party keyboards can act as key-loggers to obtain the user’s credentials.
- The app should be protected against reverse engineering.

App hardening would have raised the barrier for such an attack.

What does it mean for app providers?

- Maintain user experience
- An unprotected application/browser is an open door
- Controlling risk – not possible without application protection
- Little time for security? – SHIELD™ runs apps for you safely
- No need to change development process



THANK YOU!

VISIT US AT PROMON.CO

CONTACT:
Matthias Reichert: matthias.reichert@promon.de
+49 (0)171 2918168

promon