Product Sheet

Mobile App Shielding

wultra

Petr Dvořák
petr@wultra.com

Protecting Mobile Apps That Run Within Untrusted Environments

Protecting mobile apps that run within untrusted environments is ever more crucial as mobile become ubiquitous. Hackers and their targeted malware is an increasing threat to the mobile revolution. With the explosive growth of the mobile channel and user demand for any time/anywhere access to mobile services, app providers are challenged to keep up with security, which increases exposure to malicious attacks.

Why Wultra App Shielding?

- Defeats targeted attacks
  Wultra App Shield proactively protects your apps against zero-day and other targeted attacks, allowing mobile apps to run securely, even on highly infected devices. If hacker attacks, Wultra App Shield will respond by taking necessary measures to protect your apps fully.
- Quick to deploy
  Wultra App Shield provides an automated implementation process. Once integrated, it sifts through the business logic, event and data flows of the app, before binding itself to the existing code. This allows organizations to release protected apps quickly, without affecting the development timeline.
- Doesn’t affect user experience
  Wultra App Shield protects any mobile app for iOS and Android and it is not bound to one application with one business logic. With a minimal system overhead, it maintains an optimal user experience and app speed.
- Trusted by the European banks
  Deep protection technology used in Wultra App Shield protects mobile applications used by millions of clients of the top European banks.
- GDPR Compliance
  Protect the personal information of your customers and stay compliant with the GDPR legislation.

Solution Benefits

Wultra App Shield protects your mobile apps against following attack vectors:

- ✔ Malware
- ✔ Debugger (Java Debugger, Native debugger)
- ✔ Emulator/fake execution environment
- ✔ Cloning of the device
- ✔ Rooting/Jailbreak
- ✔ Code-Injection (prevent Runtime Library Injection)
- ✔ Hooking-Frameworks
- ✔ Repackaging (Fake, Manipulated Apps)
- ✔ System- and User-Screenshots
- ✔ Keylogging: untrusted Keyboards
- ✔ Keylogging and Screen-Scraping: untrusted Screen-readers
- ✔ Native Code-Hooks
- ✔ External Screen sharing (content being displayed 'outside' the screen of the device – for example by screen sharing).
- ✔ Man-in-the-App Scenarios
- ✔ Man-in-the-Middle Scenarios (related to network communication)
- ✔ Asset integrity checks: Wultra App Shield can perform more in-depth integrity checks of files and assets inside the APK.
- ✔ Wultra App Shield will verify the integrity of the matched files when starting the application.
- ✔ API: Foreground override detection ("Overlay- Detection") This feature detects if another application is placed in front of the currently working application in order to perform a phishing attack. This is sometimes referred to as an overlay attack, which has been widely known to be done by certain types of Android malware.
- ✔ Whitebox-Crypto features, to prevent 'important keys' from being present (and possibly stolen) in memory at any time.
- ✔ Stealing of sensitive data from the app (at rest or otherwise)

About Wultra

Wultra helps the leading European banks build secure and engaging digital channels faster. Our range of security-related software technologies covers the whole digital banking application stack, be it on the web or mobile platforms. Security solutions by Wultra secure the best mobile banking in the Czech Republic, an open banking gateway for the retail bank with over 300k clients, or a premium banking for the most affluent clientele.

Raiffeisen BANK | MONETA MONEY BANK | Equa bank | air bank