DIGIPASS® for Apps - RASP

Defeat mobile application attacks with complete protection from the inside out

Today, businesses develop and market their own mobile apps at a feverish pace, driving a significant increase in the attack surface and related fraud. At the center of this threat are hackers that release malware exploiting mobile OS vulnerabilities – injecting code into apps to modify behavior and ultimately steal data – invisible to the user. DIGIPASS for Apps – Runtime Application Self-Protection (RASP) equips businesses with strong, natively integrated application security that dynamically detects and mitigates these attacks.

SECURE SENSITIVE DATA
RASP proactively protects against zero-day and other targeted attacks, allowing mobile business apps to run securely, blocking the foreign code from working or shutting down the application if a threat to data exists. Integrating RASP into mobile apps ensures the complete integrity of the apps and fully protects sensitive business and personal data from cybercriminals.

INTEGRATED PROTECTION
RASP wraps around the application code to protect against foreign code injection. Even if a device becomes infected with malware, including system components such as screen-reader or key logging on Android, RASP technology will detect and prevent that code from running.

HOW IT WORKS
RASP ensures the integrity of mobile apps in three ways: Protect, Detect and React. It protects the trusted mobile application by preventing reverse engineering techniques via code obfuscation and anti-repackaging technology.

It actively detects malicious key logging, screen readers, repackaged applications, debuggers and emulators, and jailbroken or rooted devices. It can then react to prevent screenshots, block screen duplication, or enable customized actions based on business policy (i.e. Application shut down).

STRENGTHEN APPLICATION SECURITY
RASP provides an extensive list of features that are easy to integrate and invisible to the end user. As a result, RASP allows businesses to extend and strengthen application security, protect customers and meet aggressive application development timelines.
RUNTIME APPLICATION SELF-PROTECTION INCLUDES

- Overlay Detection
- Jailbreak & Root Detection
- Active Memory Zeroing
- Secure Storage + Device Binding
- Anti-Code Injection
- Anti-Key Logging
- Anti-Screen Reader
- Anti-System Screen shots
- Anti-Screen Mirroring and External Monitors
- Anti-Re-Packaging Protection
- Debugger & VM Debuggers Prevention
- Runtime Protection—Integrity Check
- Emulator Detection
- Obfuscation

TECHNICAL SPECIFICATIONS

RASP supports iOS as of version 6.0 that needs to be linked to a host application. The framework is currently provided for the following architectures:

- armv7
- armv7s
- arm64
- i386
- x86_64

RASP supports Google Android 2.3 and later. The following CPU architectures are currently supported:

- armeabi
- armeabi-v7a
- armeabi-v8a
- mips
- x86
- x86_64

About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security and designs, develops, markets and supports DIGIPASS®, CertiID™, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products. VASCO’s prime markets are the financial sector, enterprise security, e-commerce and e-government.

www.vasco.com