

Highlights

- Gain visibility into security and privacy risks of mobile apps
- Assess internally developed and third-party mobile apps
- Leverage scale and cost advantage of automated solution
- Learn about expert advice on effective remediation and mitigation strategies



Mobile App Security and Privacy Analysis

By some estimates the worldwide mobile industry is well on its way to achieving 44 billion cumulative downloads of mobile apps by 2016. CISOs and security professionals are taking note of the increasing popularity of smartphones and tablets and the proliferation of customer-facing and corporate-oriented mobile apps. As these apps start to access sensitive data and transact business critical operations, questions about their inherent security and privacy posture need to be answered. While a mobile workforce stands to enhance productivity it should not come at the expense of security and privacy. Veracode's Mobile App Security and Privacy Analysis service helps customers learn about the security risks and potential privacy violations of internally developed and third-party mobile applications.

Knowledge is Power: Know the 'Nutrition Label' for Your Mobile Apps

Fears abound amongst those responsible for corporate security and risk on the unfettered use of mobile devices and applications. These fears are well justified. Mobile apps provide a uniquely portable risk factor, combining applications of unknown origin with close access to sensitive data in a highly portable, highly networked platform. Despite these concerns little exists by way of real data, to help security and risk professionals knowledgeably guide the business or make informed decisions about their mobile security strategy.

Veracode's Mobile App Security and Privacy service was designed to empower customers with real knowledge about the security risks and potential privacy concerns that lurk in mobile apps they are developing internally or purchasing from third-party app stores and developers. Veracode has extended its patented and proven static binary analysis technology to provide unique coverage for mobile apps. As with non-mobile applications, customers or third-parties upload their final integrated applications to the cloud platform. Veracode performs automated analysis to discover both traditional security issues such as buffer overflows as well as security and privacy issues specific to the mobile computing environment such as data exfiltration flaws.

The resulting report provides customers with a deep behavioral analysis, a 'nutrition label', for their mobile app which allows them to understand the potential risk posed by its use within their organization. Specific guidance is also provided on how to remediate these flaws. Unlike mobile app whitelisting solutions that identify 'known' bad apps Veracode's service helps customers identify previously unknown security and privacy issues in their mobile apps.

Supported Platforms

Veracode supports the following mobile platforms for static binary scanning.

PLATFORM	VERSION
Android	API level 8, 9 (Android 2.2, 2.3), Applications should be fully implemented in Java
BlackBerry	J2ME
Windows Mobile	Windows Mobile 6.0, 6.1

Please refer to Veracode compilation guide for other technical specifications related to the service. **iOS 4.2, 4.3 (universal apps only, compiled with gcc) will be supported in June 2011.** iOS applications should consist of C/C++ and Objective-C only. Applications containing code in other languages (e.g. Lua, Scheme, JavaScript, Flash, etc.) are not supported.

Mobile Security Issues: A Multi-tiered Challenge

Mobile applications may have several types of security risk: language inherent risk, based on common security flaws in the language; malicious data exfiltration, in which sensitive data is surreptitiously transmitted from the phone; and platform specific risk, based on specific vulnerabilities inherent in the mobile platform. Some examples of the types of language related and other flaws that Veracode's automated service discovers for mobile apps are discussed below.

Language Specific Flaw Categories

Mobile applications inherit a certain amount of risk from the languages in which they are written. While some of this risk may be mitigated by the runtime environment in which the applications are deployed, there may still be threats to the confidentiality, integrity, or availability of the application and the data that it accesses from flaws of this kind. Examples of the types of language-related flaws that Veracode's scans may detect include:

- Cryptographic Flaws
- Buffer Overflows
- Credentials Management
- Numeric Flaws
- Code quality
- Information Leakage

Malicious Data Exfiltration flaws

Mobile data exfiltration is defined as the deliberate dissemination of sensitive information from a mobile handheld device to a third party via common data transmission methods. Based in Veracode's groundbreaking work on malicious data exfiltration in conventional applications, the primary goal of the malicious data exfiltration scan is to determine if a piece of mobile binary code presents a risk via deliberate data disclosure. Examples of the kinds of malicious behavior that Veracode's scans may detect include:

- Deliberate transmission of address book data, email, phone log, or SMS
- Surreptitious transmission of microphone, GPS, or camera data
- Exfiltration via sockets, e-mail, HTTP, SMS, DNS, ICMP, IR



Veracode, Inc.
4 Van de Graaff Drive
Burlington, MA 01803
Tel +1.781.425.6040
Fax +1.781.425.6039
www.veracode.com
© 2011 Veracode, Inc.
All rights reserved.

ABOUT VERACODE

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. By combining patented static, dynamic and manual testing, extensive eLearning capabilities, and advanced application analytics Veracode enables scalable, policy-driven application risk management programs. Veracode delivers unbiased proof of application security to stakeholders across the software supply chain while supporting independent audit and compliance requirements for all applications no matter how they are deployed, via the web, mobile or in the cloud. The company's more than 175 customers include Barclays PLC, California Public Employees' Retirement System (CalPERS), Computershare and the Federal Aviation Administration (FAA). For more information, visit www.veracode.com, read the ZeroDay Labs' blog or follow on Twitter @Veracode.