CENSUS
IT Security Works

MOBILE APP TESTING

WHAT IS MOBILE APP TESTING?

The ecosystem that surrounds mobile apps is affected by a growing number of threats. App users may fall victims of malware that "steal" sensitive, but unprotected, app data. App services may be compromised by the remote exploitation of bugs in the app web API. Businesses may experience significant losses in revenue by the wide-spread use of modified (repackaged) versions of their apps, versions that are lacking critical functionalities such as in-app advertisements.

Mobile App Testing is a software assessment process that is specially designed to identify security issues in mobile applications and related services. For apps that are under development, Mobile App Testing allows for the early detection of security risks and the production of high quality releases. For apps that have already been released, Mobile App Testing provides unique insights into the risks associated with the use of these apps and their related services.

THE CENSUS MOBILE APP TESTING METHODOLOGY

CENSUS offers Mobile App Testing services for applications of all major platforms (iOS, Android, Windows Phone, Blackberry OS and HTML5). To quickly identify all types of security issues affecting an application, CENSUS uses a methodology which utilizes multiple analysis techniques: App Static Analysis, App Dynamic Analysis, API Testing, Third Party Code Assessments and App Bundle Inspection.

The CENSUS Mobile App Testing methodology is designed to be fully compatible with the requirements set by Secure Software Development strategies. To further support such strategies, CENSUS also offers training courses for the secure development of mobile applications and the realization of a Secure Software Development Lifecycle.

APP STATIC ANALYSIS

During Static Analysis, CENSUS experts examine the mobile app's source code (or the recovered, through reverse engineering, code if source code is not available) line-by-line in order to identify security vulnerabilities. Static Analysis is unique in that it can reveal all types of security issues, even business logic ones, as it maps the full internal structure of the application and its use of external libraries and services. Static Analysis can also be applied to web APIs (or other APIs and services that the app uses) when the source code for these has been made available for auditing purposes.

APP DYNAMIC ANALYSIS

During Dynamic Analysis, the mobile application's runtime behavior is examined to identify security issues caused by the application's interaction with platform and external services, but also to verify security issues caused by complex conditions in the program code. Dynamic Analysis requires a live testing environment, if the application communicates with external services as part of its operation.

API TESTING

API Testing is a similar testing process to App Dynamic Analysis, but instead of identifying issues on the mobile application, it identifies security issues on external services (APIs) that the application uses. During API Testing, CENSUS experts perform a live security analysis of all API states of a service, as well as a Penetration Test to verify that the service operates on a properly secured application stack.

THIRD PARTY CODE ASSESSMENTS

CENSUS performs a pre-release vulnerability assessment to third party code and libraries used by a mobile application, to identify known security weaknesses in these, that would also affect the released app. At the client's request, CENSUS can also perform Vulnerability Research on third party software (for which the source code may or may not be available) to identify previously unknown weaknesses (i.e. "0-day" vulnerabilities).

APP BUNDLE INSPECTION

During App Bundle Inspection, CENSUS experts check whether the app has been built and packaged correctly prior to its publishing to the app store. This testing procedure ensures that no debugging or sensitive information have made it into the app bundle, that all security controls (including binary protection mechanisms) operate as expected and that no security issues arise from the app's build time configuration.

ISSUE REPORTING

Issues are documented either in the form of a technical report or as an issue tracker spreadsheet based on a client selected scoring system (e.g. CVSS). Both report and tracker describe the identified security vulnerabilities in detail, evaluate their respective risks and propose mitigations for these risks. Issues can also be documented on a bug reporting system designated by the client.

CENSUS experts remain at the client's service for issue retesting and consulting regarding the handling of open issues.

BENEFITS

Mobile App Testing allows for the early mitigation of risks, providing the best possible protection for businesses, services and users of mobile applications.

CENSUS offers comprehensive Mobile App Testing services to customers worldwide, based on years of experience and research in the field of mobile application security. Building on this knowledge base, CENSUS experts go well beyond the identification of standard issues (e.g. OWASP Mobile Top 10 Risks), revealing also vulnerabilities that are due to the application's interaction with 3rd party technologies (e.g. MDM, binary protection solutions) or due to its execution on specific platforms and devices.

For more information about the CENSUS Mobile App Testing services please visit: **www.census-labs.com**

CENSUS
IT Security Works

www.census-labs.com

USA
607 Boylston Street,
Suite 165L, Boston, MA 02116
T. +1 617-448-5050
E. usa@census-labs.com

EUROPE
128, Leoforos Andrea Syggrou,
11745, Athens, Greece
T. +30 210 220 8989-90
E. eu@census-labs.com

UK
4th floor, The Pinnacle,
Station Way, Crawley RH10 1JH
T. +44 (0) 1293 763 336
E. uk@census-labs.com