Service Definition
Mobile App Security Assessment

Introduction

With the rise of mobile working via Android, iPhone, iPad and Windows mobile devices, there are an increasing number of methods to gain access to corporate information. What if these devices are infected, lost, stolen, misused or simply misconfigured? A security assessment of the deployment can help answer those questions and reduce security exposure.

The objective of Intertek NTA's Mobile App Security Assessment service is to ensure that devices are securely configured, thus preventing an attacker from gaining access to corporate data via a lost or stolen device, and preventing an authorised mobile user from gaining access to any restricted functionality or data assets.

This service allows organisations who have procured services via the Digital Marketplace, or who are using cloud hosted software, infrastructure or platforms, to gain independent analysis and information security assurance regarding the governance and controls that are in place to protect these services and systems. Such assurance is vital for cloud based services which possess specific security considerations due to their on-demand, remotely accessible and multi-tenanted attributes.

This specialist testing service provides customers with governance support in relation to the integration of cloud based services and systems into their organisations.

Scoping

A scoping conversation will be held prior to delivery to identify the target devices and operating system versions, and to discuss any particular areas of concern. A recommended number of units/days will then be provided to enable requirements to be met.

Service Overview

This service may be purchased either individually or as a collection of services offered by Intertek NTA.

Largely based on Intertek NTA’s Web Application Security Test service, the Mobile App Test will check that the mobile version of web sites are secure. Developers often neglect the security side of mobiles sites assuming that it's going to be used on a mobile rather than a PC. For example, instances in which injection is rejected on a web application, can often not adhere to the same injection sanitisation when tested on the mobile application.

Intertek NTA’s Mobile application testing provides an in-depth security assessment of your mobile application, including both Android and Apple iOS applications. The objective is to ensure that the application is securely configured, thus preventing an attacker from bypassing access restrictions, escalating user privilege, and gaining access to the underlying data stored within the local database.

As a minimum, testing will encompass the top ten issues as defined by the OWASP Mobile Security Project. The key areas covered will include:

- M1: Improper Credential Usage
- M2: Inadequate Supply Chain Security
- M3: Insecure Authentication/Authorization
- M4: Insufficient Input/Output Validation

- M5: Insecure Communication
- M6: Inadequate Privacy Controls
- M7: Insufficient Binary Protections
- M8: Security Misconfiguration
- M9: Insecure Data Storage
- M10: Insufficient Cryptography

Key areas of consideration will include:

Local Data Storage
The protection of sensitive data, such as user credentials and private information, is crucial to mobile security. If an app uses operating system APIs such as local storage or inter-process communication (IPC) improperly, the app might expose sensitive data to other apps running on the same device. It may also unintentionally leak data to cloud storage, backups, or the keyboard cache. Additionally, mobile devices can be lost or stolen more easily compared to other types of devices, so it's more likely an individual can gain physical access to the device, making it easier to retrieve the data.

Communication with Trusted Endpoints
Mobile devices regularly connect to a variety of networks, including public Wi-Fi networks shared with other (potentially malicious) clients. This creates opportunities for a wide variety of network-based attacks ranging from simple to complicated and old to new. It's crucial to maintain the confidentiality and integrity of information exchanged between the mobile app and remote service endpoints.

Authentication and Authorisation
In most cases, sending users to log in to a remote service is an integral part of the overall mobile app architecture. Even though most of the authentication and authorisation logic happens at the endpoint, there are also some implementation challenges on the mobile app side. Unlike web apps, mobile apps often store long-time session tokens that are unlocked with user-to-device authentication features such as fingerprint scanning. While this allows for a quicker login and better user experience, it also introduces additional complexity and room for error.

Interaction with the Mobile Platform
Mobile operating system architectures differ from classical desktop architectures in important ways. For example, all mobile operating systems implement app permission systems that regulate access to specific APIs. They also offer inter-process communication (IPC) facilities that enable apps to exchange signals and data. If IPC APIs are misused, sensitive data or functionality might be unintentionally exposed to other apps running on the device.

Code Quality and Exploit Mitigation
Traditional injection and memory management issues aren't often seen in mobile apps due to the smaller attack surface.

Mobile apps mostly interact with the trusted backend service and the UI, so even if many buffer overflow vulnerabilities exist in the app, those vulnerabilities usually don't open up any

useful attack vectors. The same applies to browser exploits such as cross-site scripting (XSS), however are still theoretically possible.

Deliverables
The output is a tailor-written formal report containing:

- An executive overview with business implications
- A summary of risks identified, ordered from high to low severity
- Technical details of each issue found
- Recommendations for closing holes found
- Full listing of test results tables including background information/evidence to support results

The style and format of the report is designed with clarity and ease of use in mind. Features include hyperlinks to relevant sections of the document as well as external sources where applicable.

A technical telephone debrief is available and included as standard following delivery of the report, to explain the areas covered during the assessment and the key findings and potential business implication (severity) of the issues found. This will include suggested priorities for the customer to take action against.

Service Management
You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

Intertek NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, Intertek NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling the test, ensuring reports are sent out in a timely manner, scheduling follow up tests and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

Ordering and Invoicing Process
Once the scope of work and number of units/days required has been agreed between the customer and Intertek NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

Customer Responsibilities

Service Definition
Mobile App Security Assessment

The customer is responsible for the completion of a Technical Details Form (TDF) prior to delivery. The provision of appropriate information, such as the device itself plus associated login credentials, will ensure that delivery meets expectations and requirements. Intertek NTA will then be responsible for returning the device once the service has been successfully completed.