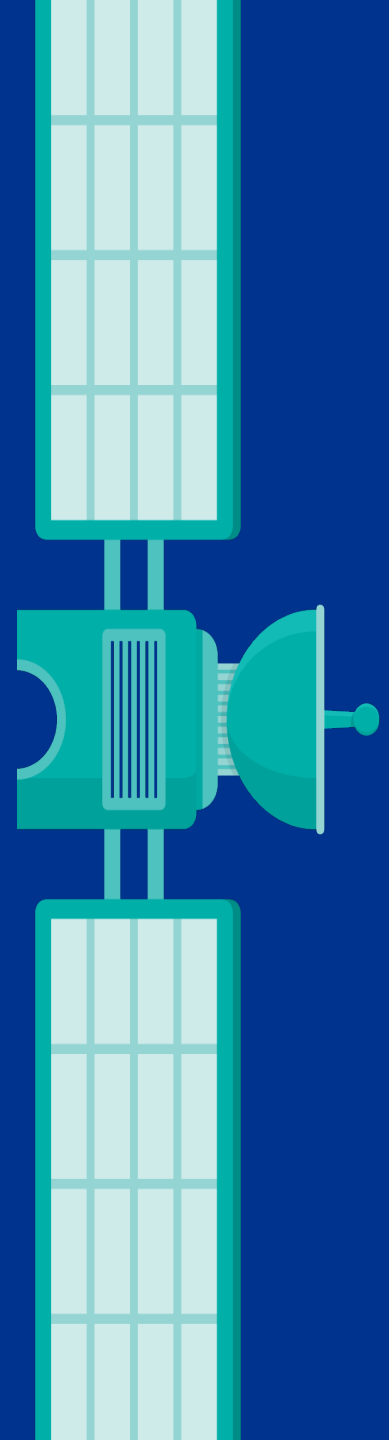
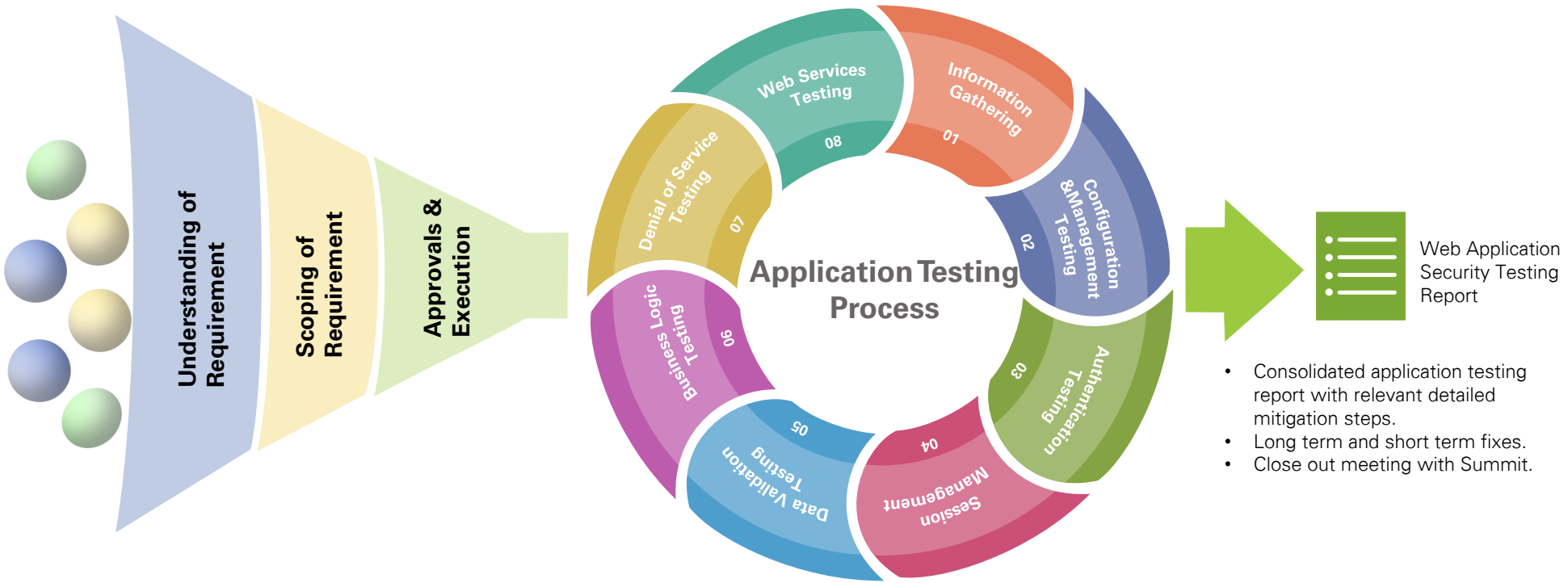
KPMG

Application Security Assessment



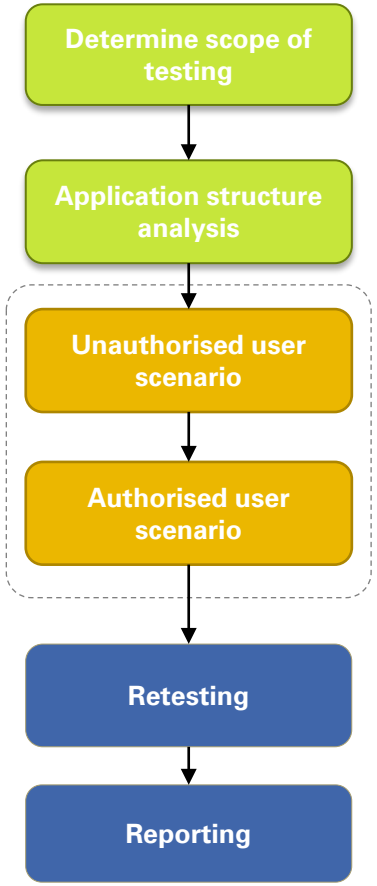
Web Application Security Testing

The KPMG approach to application security testing : Each application and environment is unique, however, KPMG has developed a unified methodology that addresses the requirements of application security testing. The KPMG methodology for application security testing includes a dual approach which covers automated as well as manual approach:



- Consolidated application testing report with relevant detailed mitigation steps.
- Long term and short term fixes.
- Close out meeting with Summit.

Web Application Security Testing - Methodology



The KPMG approach to Application security testing

Each application and environment is unique, however, KPMG has developed a unified methodology that addresses the requirements of application security testing. The KPMG methodology for application security testing includes a dual approach:

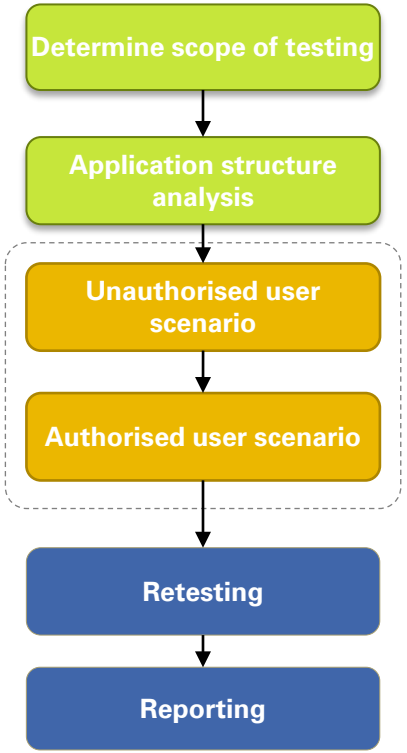
Unauthorized User Scenario:
This is an initial examination of the application to assess the access privileges , actions and transaction processing capabilities that are exposed to an unauthorized user. This test simulates the type of action an external attacker would use to subvert security controls.

Authenticated User Scenario:
Analysis of possibility of escalation of assigned privileges, arbitrary code execution and exploitation of vulnerabilities leading to access to the underlying infrastructure is performed. This requires authorized user credentials with different privilege levels on the application.

API Security Testing

External hackers that can compromise the security of a remote application are frequently in a position to launch a further attack from the trusted side of a firewall, potentially with access to internal databases and systems. All too often these attacks are carried out with little more than a web browser and will go un-noticed by many current intrusion detection systems.

Our approach is based on the latest version of the leading web security industry standard “OWASP Testing guide” complimented by KPMG’s proprietary security testing process.



API Security Testing

The KPMG approach to API/Protocol security testing

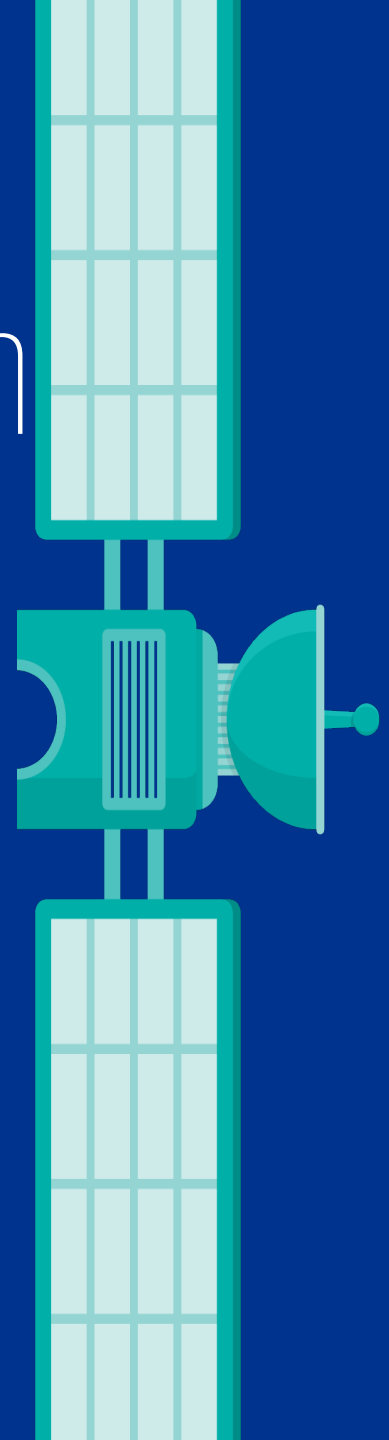
Each application and environment is unique, however, KPMG has developed a unified methodology that addresses the requirements of application security testing. The KPMG methodology for application security testing includes a dual approach:

Unauthorized User Scenario:
This is an initial examination of the application to assess the access privileges , actions and transaction processing capabilities that are exposed to an unauthorized user. This test simulates the type of action an external attacker would use to subvert security controls.

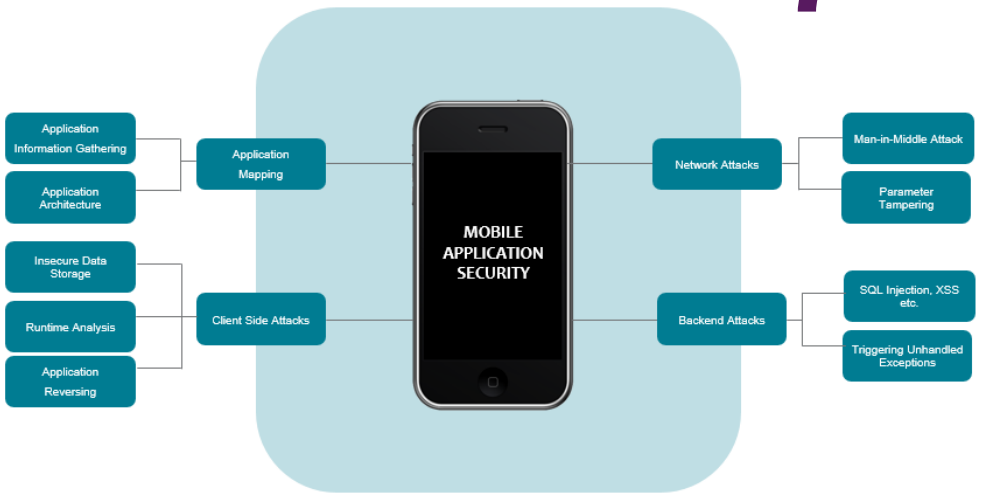
Authenticated User Scenario:
Analysis of possibility of escalation of assigned privileges, arbitrary code execution and exploitation of vulnerabilities leading to access to the underlying infrastructure is performed. This requires authorized user credentials with different privilege levels on the application.

KPMG

Mobile Application Security Approach



Mobile Application Security Approach



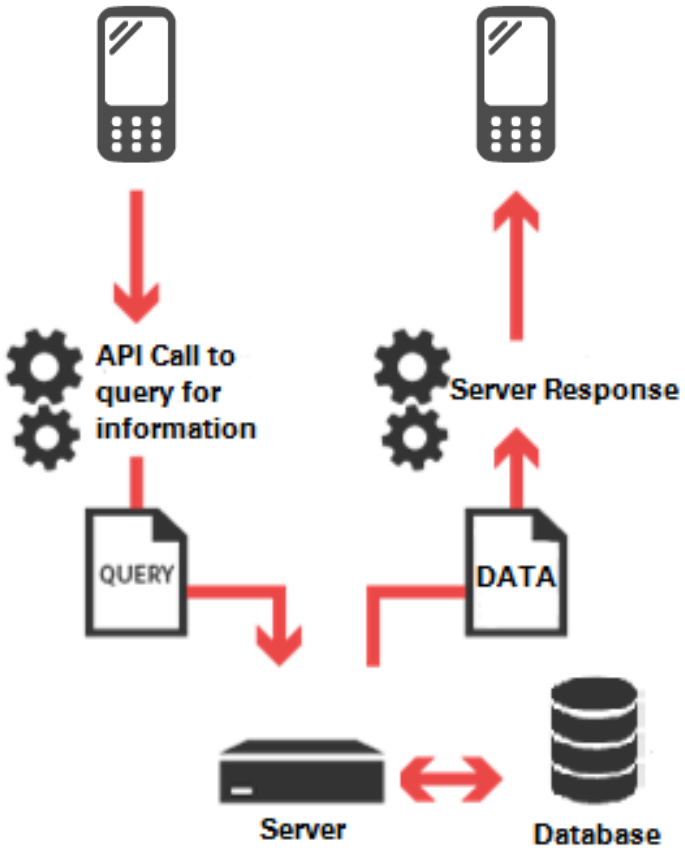
Key vulnerabilities / standards considered during mobile application security assessments

OWASP Mobile Top 10 2017	
M1 Improper Platform Usage	M6 Insecure Authorization
M2 Insecure Data Storage	M7 Client Code Quality
M3 Insecure Communication	M8 Code Tampering
M4 Insecure Authentication	M9 Reverse Engineering
M5 Insufficient Cryptography	M10 Extraneous Functionality

KPMG's Mobile Application Security Assessment model is based around client-side security where an end-user is in control of his device and is responsible for securing his computer against attacks with the service provider only offering hints or free software. In mobile application environments, end-users may not always be aware of the threats they are facing and may not be in complete control of the device. Additionally, most mobile web applications are bespoke and for single purpose and typically do not benefit from the "many eyes" advantage a popular software product receives. To address these, KPMG also incorporates an end-user application security review process.

KPMG's Mobile Security Assessment Services will help you understand your mobile application security posture with respect to both internal and external attacks better.

Mobile Application Security Assessment Methodology



Client Side Attacks
- The client application is tested either using a platform emulator typically provided together with SDK and / or actual hardware device
- Insecure Data Storage checks on the applications
- Functionality of the client application thoroughly analyzed to identify assumptions about platforms of execution that may not be always true, for example: an application relies on GPS data being accurate, then such data might be spoofed if the application is executed on an emulator.

TIER 1

Communication Channel Attacks
The data exchange between client-side application and server-side application is intercepted using various tools and client-side application is being supplied with invalid responses to trigger erroneous behavior. Fuzzing tools are used where possible to cover maximum attack surface followed by manual investigation of suspicious behavior.

TIER 2

5.

Backend and Server Side Attacks
-Application Administrator portal facing either the internal / external network are investigated
-The server-side security testing is carried out using one of the approaches described in the application security assessment methodology: black box, grey box and white box approach.

TIER 3