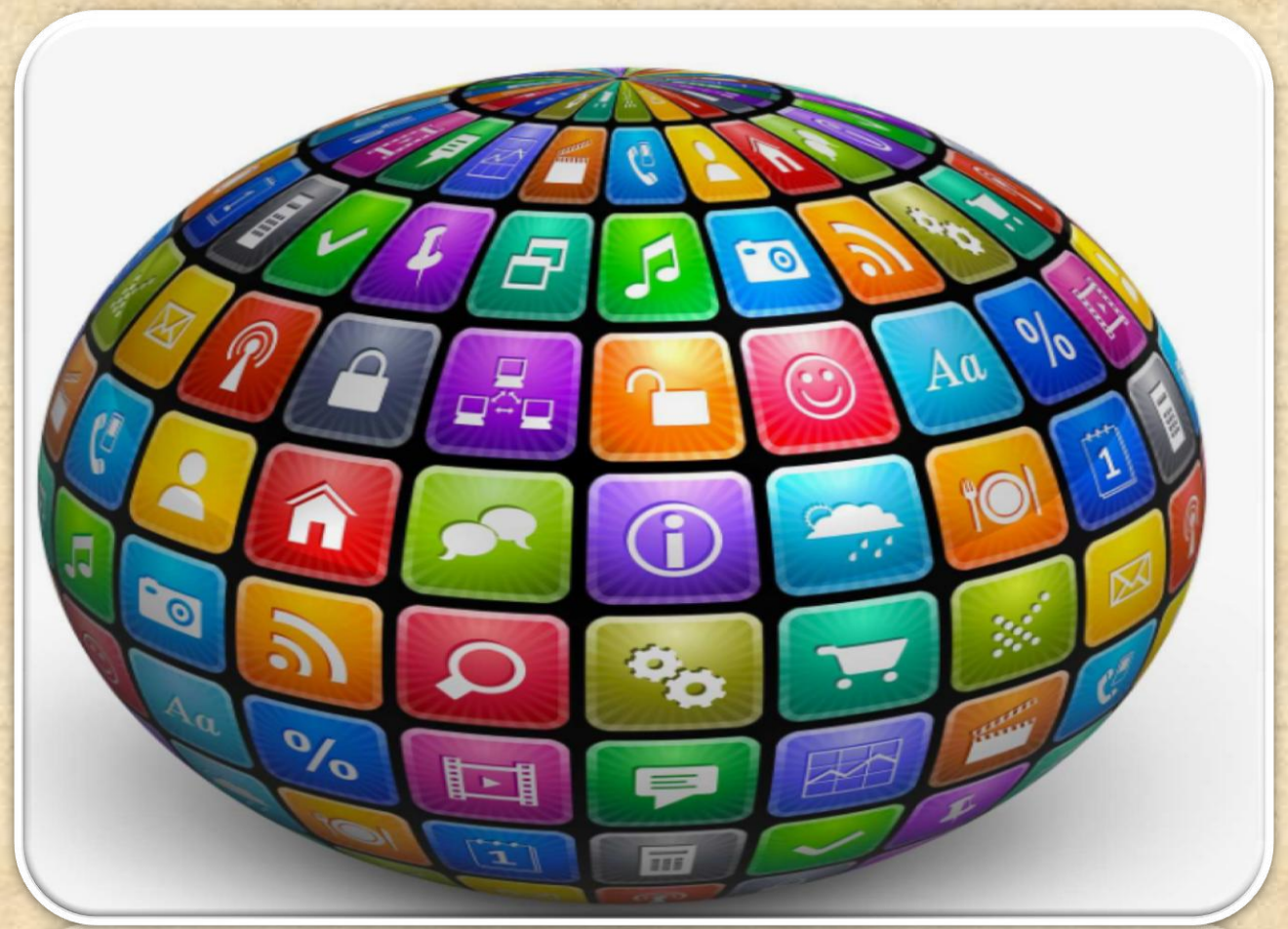
Becoming a Pro

IN Mobile Applications Testing



Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

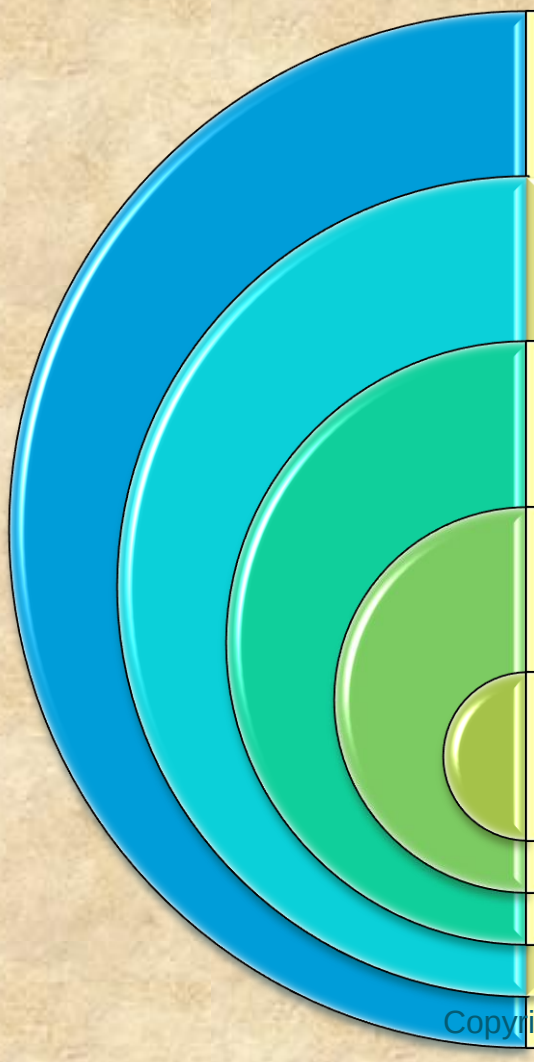
Platform/OS TEST

- Different OS ->Android, IOS, Windows
- Different browsers -> Firefox, Google Chrome, IE, Safari
- Different Screen Size and resolution
- OS versions and memory size
- Hardware capable of interrupt handling without getting hanged
- Multilingual Support
- Different Time Zones Support

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps EXTRA

ACCESSIBILITY TEST (What is SCREEN READER ?)



Mobile Accessibility is critical to reaching all audiences. A product is accessible when a person with a disability can have an experience equivalent to that of a person without a disability

Users who are blind will use a screen reader to navigate and access information on mobile devices.

The screen readers are included in the device operating system and can be turned on in the device settings.

When Screen Reader is turned on, the gestures and keyboard shortcuts change.

In the 2014 Webaim survey shows that 82% of Screen Reader users will use a mobile device

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps EXTRA

ACCESSIBILITY TEST (SCREEN READER)

Web Content Accessibility Guidelines (WCAG)

- A person who is blind using a screen reader or a talking browser can navigate your information and interact with it.
- A person with low-vision can magnify the screen and understand the content.
- A person who is deaf or hard-of-hearing can read captions in multimedia presentations.
- A person with a dexterity limitation can use the alternative input devices for all interaction, or can use speech recognition software.
- A person with ADHD or dyslexia can use and understand the content and complete tasks
- Please refer to this link to learn more https://www.w3.org/TR/WCAG20/

- Screen reader testing on mobile
- Zooming site/application
- Color ratios
- Readability of the site
- Navigation

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA

Workshop : ANSWER THESE QUESTIONS

1. *What do you consider to be the biggest security issues with mobile phones?*
2. *How seriously are consumers and companies taking these threats?*
3. *What can be done about these threats?*

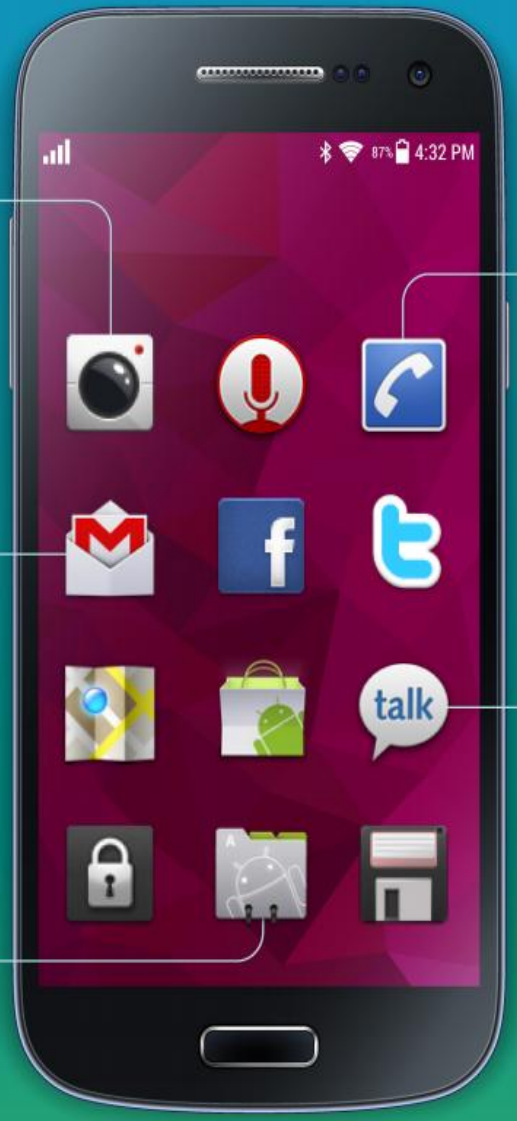
Mobile Test Industry Standards :

Ways your Device might be compromised by a hacker ?

Surveillance
- Record audio
- Camera, photos and videos
- Location
- Call history
- Text messages

Impersonation
- SMS redirection
- Sending emails
- Posting to social media

Data Theft
- Account logins and passwords
- Contacts, phone number and call history
- Steal International Mobile Equipment Identity (IMEI) number



Financial
- Send premium rate SMS messages
- Make expensive phone calls
- Steal Transaction Authentication Numbers (TAN)
- Extort you via ransomware and fake antivirus

Botnet Activity
- Click fraud
- Send premium rate SMS
- Launch Distributed Denial of Service (DDoS) attacks

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA

- Attacks on mobile devices range in volume and severity, but all have the potential to cause chaos at both a device and network level.

Just like in the conventional fixed Internet world, attacks come in all shapes and sizes – such as:

- Phishing (criminals attempt to trick users into sharing passwords etc)
- Spyware (tracks user's activity, perhaps selling data to advertisers)
- Worms (a program that copies itself onto multiple devices via network connections)
- Trojans (a program that looks genuine but hides malicious intent)
- Man-In-The-Middle Attacks (where a criminal intercepts and manipulates messages between two devices or device and computer).

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

OWASP Mobile Security Project

Security Test EXTRA

What is OWASP ?

- The Open Web Application Security project is an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of Web App Security

OWASP Top Ten:

- The Top Ten was first published in 2003 and is regularly updated.
- Its goal is to raise awareness about application security by identifying some of the most critical risks facing organizations.
- The Top 10 project is referenced by many standards, books, tools, and organizations, including MITRE, PCI DSS, Defense Information Systems Agency, FTC, and many more.

CWE – COMMON WEAKNESS ENUMERATION :
https://cwe.mitre.org/about/

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

There are two main categories of mobile code security risks:

MALICIOUS FUNCTIONALITY

- The category of malicious functionality is a list of unwanted and dangerous mobile code behaviors that are stealthily placed in a Trojan app that the user is tricked into installing.
- Users think they are installing a game or utility and instead get hidden spyware, phishing UI or unauthorized premium dialing.

VULNERABILITIES.

- The category of Mobily Security vulnerabilities are errors in design or implementation that expose the mobile device data to interception and retrieval by attackers.
- Mobile code security vulnerabilities can also expose the mobile device or the cloud applications used from the device to unauthorized access.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN 2017

- A1-Injection
- A2-Broken Authentication and Session Management
- A3-Sensitive Data Exposure
- A4-XML External Entities (XXE)
- A5-Broken Access Control
- A6-Security Misconfiguration
- A7-Cross-Site Scripting (XSS)
- A8-Insecure Deserialization
- A9-Using Components with Known Vulnerabilities
- A10-Insufficient Logging&Monitoring

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test

CREATE CHECK LIST BEFORE

- Phone identifiers such as (IMSI or IMEI)
- Address Book
- Account Details
- E-maiL
- Stock application data
- Banking Data
- GPS Location(s)
- Web History
- User's Dictionary
- Images
- Notes
- Calendar Appointments
- Call Logs
- Encryption Keys

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps EXTRA

SUMMARY

Functional
- Validation of Functionality
- Smoke / Regressions Testing
- Offline access testing
- Negative Testing

Non Functional
- Network Strength / Outage / Recovery
- Different NW Types
- Peripheral Testing

Interoperability (IOP)
- Voice / SMS interrupts
- Notifications
- Battery /Cable Removal

Memory Leak
- Memory Usage
- Memory Leaks
- Garbage Collection

Performance Testing
- CPU Usage testing
- Network Usage
- Page Render time or activity Render time

Usability Testing
- User Experience
- Competitive Analysis
- Expert Review

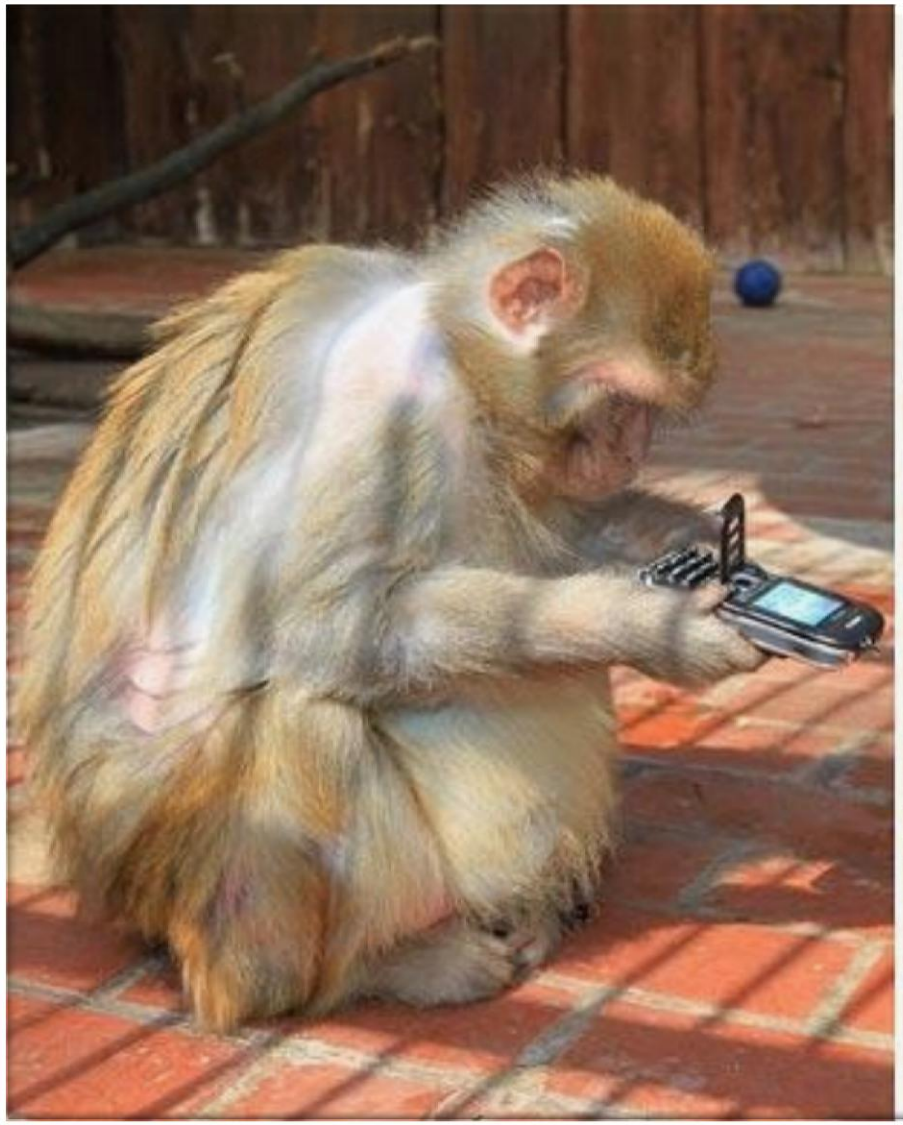
Installation Testing
- New App Install
- Uninstall and **Reinstall**
- Upgrade testing

Security Testing
- OWASP Vulnerabilities
- Dynamic Testing
- Static Code Analysis
- Data Encryption

Language Testing
- Validation for Locales
- Images and Text
- Currencies, time zones etc.
- Context

Mobile Test Industry Standards

Testing Strategies for Mobile Apps : LETS PRACTICE



Mobile Test Industry Standards

Testing Strategies for Mobile Apps : LETS PRACTICE

How to Start Testing a Mobile Page

Find and divide page into components/modules → Create a list/table of modules/testing types/ testing → Create a variety of variables and conditions within each module → Specify the Expected and leave place for Actual Results

FOR TROUBLESHOUTING Create a list/table to view ANY problem from different angels → Create a Check List for Testing Categories: → Functionality Testing → Usability testing

Interruption testing → Connectivity testing → Compatibility testing → Performance testing

Security testing

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

GUI TEST Checklist

- Navigation
- Formatting
- Color and fonts
- Scrolls
- Controls and alignments
- Spelling and grammar
- Justification
- Look and feel
- Default and shortcut keys
- Tab
- Opening input
- Alternatives
- Behavior
- Modality and multiple windows
- Contrast
- Images

Mobile Test Industry Standards

Testing Strategies for Mobile Apps : LETS PRACTICE

top considerations for creating a release CHECK LIST for mobile app testing

- Application Installation/Update
- Application Sign Up & Log in
- Subscription scenarios
- Application Sanity Suit
- APP works in different Mobile modes
- User Friendly
- Network connectivity
- Data save conditions
- Mobile interruptions
- Battery Consumption
- Mobile memory utilization
- Mobile data utilization
- Screen scrolling application screen
- New OS release support
- correct implementation of AdMob or other mobile ad platform

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Smoke and Sanity TEST Checklist –UI

1. APP/Webpage title as per the page's functionality.

2. Spelling/ grammatical mistake (e.g. Text, Caption, Label).

3. Proper field alignment (Left margin, right margin, bottom margin, top margin).

4. Same font size/style or as per the requirement.

5. Proper space between texts, text lines, fields.

6. Standard format and size of button.

7. Textbox: Border, alignment, size, length, Data Type.

8. Combo box: Size, alignment, showing valid value.

9. Date picker (Not by keyboard, from date to date range).

10. Mandatory field identified with an identification like (*) sign.

11. Image length, size, alignment

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Smoke and Sanity TEST Checklist –Functional

1. Mandatory and composite field validation.

2. Error message not mandatory for optional field.

3. Numeric field does not accept the alpha numeric and proper error message display.

4. Max length checking for specific input field (e.g. Credit card number, Account number).

5. Confirmation message for Insert/update/ delete operations.

6. Correct format of amount value.(Should be numeric)

7. Uploaded documents are opened and generated properly.

8. Validation (Equivalence partitioning/Boundary value analysis/Positive testing/Negative/Page Refreshing).

9. System works properly with multiple browsers.

10. Pagination works and number shows properly.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Smoke and Sanity TEST Checklist –Database

1. Database name, Tables, columns name, column types matches according to requirement.

2. Data saves properly into the database after the each page submission.

3. Data display on the front end and make sure it is same in the back end.

4. Is any difference between Live and Test environment (Database Name, Table Name, Column Name, Data Type, Entity Relationship Key – Primary, Foreign, Unique key)

5. Checking Procedure/Function Create/Update related information(Entity Name, Author, Create/Update Date, Description/Purpose)

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Smoke and Sanity TEST Checklist –Security

1. Session timeout checking. Whether the page is expiring after the specific time.

2. Does the page browse if I paste it in a newly open browser?

3. Browser back-forward button checking if the page consist any calculation or information submission.

4. Does the browser's back-forward button re-submit the page?

5. Does this application has admin/user log in the database?

6. Password, Account number, credit card number display in encrypted format.

7. Access the secured App/web page directly without login

8. User account gets locked out if the user is entering the wrong password several times.